BASES ESTÁNDAR DE LICITACIÓN PÚBLICA PARA LA CONTRATACIÓN DE BIENES

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

OSCE Organismo Supervisor de las Contrataciones del Estado

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

SIMBOLOGÍA UTILIZADA:

N°	Símbolo	Descripción
1	[ABC] / [.....]	La información solicitada dentro de los corchetes sombreados debe ser completada por la Entidad durante la elaboración de las bases.
2	[ABC] / [.....]	Es una indicación, o información que deberá ser completada por la Entidad con posterioridad al otorgamiento de la buena pro para el caso específico de la elaboración de la PROFORMA DEL CONTRATO; o por los proveedores, en el caso de los ANEXOS de la oferta.
3	**Importante** • *Abc*	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	*Advertencia* • *Abc*	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	**Importante para la Entidad** • *Xyz*	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y deben ser eliminadas una vez culminada la elaboración de las bases.

CARACTERÍSTICAS DEL DOCUMENTO:

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

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

INSTRUCCIONES DE USO:

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

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

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

BASES ESTÁNDAR DE LICITACIÓN PÚBLICA PARA LA CONTRATACIÓN DE BIENES

LICITACIÓN PÚBLICA Nº 17-2022-INEN

PRIMERA CONVOCATORIA

ADQUISICIÓN DE SOLUCIÓN DE PROTECCIÓN DE VIRUS INFORMATICOS

DEBER DE COLABORACIÓN

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

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

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

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

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I
ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

Importante

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

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

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

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

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

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

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

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

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

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

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

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

1.9. EVALUACIÓN DE LAS OFERTAS

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

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

1.10. CALIFICACIÓN DE OFERTAS

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

1.11. SUBSANACIÓN DE LAS OFERTAS

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

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

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

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 y el otorgamiento de la buena pro.

1.14. CONSENTIMIENTO DE LA BUENA PRO

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

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

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

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

CAPÍTULO II
SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

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

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

Importante

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

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

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

- *El recurso de apelación se presenta ante la Mesa de Partes del Tribunal o ante las oficinas desconcentradas del OSCE.*

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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

CAPÍTULO III
DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

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

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 bienes, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del funcionario competente.

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

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

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

3.9. DISPOSICIONES FINALES

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

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I
GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre	:	**INSTITUTO NACIONAL DE ENFERMEDADES NEOPLASICAS**
RUC Nº	:	**20514964778**
Domicilio legal	:	**AV. ANGAMOS ESTE N° 2520-SURQUILLO**
Teléfono:	:	**201-6500 ANEXO N° 1176**
Correo electrónico:	:	wfernandez@inen.sld.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la ADQUISICIÓN DE SOLUCIÓN DE PROTECCIÓN DE VIRUS INFORMATICOS.

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Resolución Directoral N°00152-2022-GG/INEN el 21 de octubre de 2022.

1.4. FUENTE DE FINANCIAMIENTO

-Recursos Ordinarios
-Recursos Directamente Recaudados
-Donaciones y Transferencias

1.5. SISTEMA DE CONTRATACIÓN

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

1.6. MODALIDAD DE EJECUCIÓN

NO CORRESPONDE.

1.7. DISTRIBUCIÓN DE LA BUENA PRO

NO CORRESPONDE.

1.8. ALCANCES DEL REQUERIMIENTO

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

1.9. PLAZO DE ENTREGA

Los bienes materia de la presente convocatoria se entregarán de la siguiente manera:

- **Plazo de la prestación principal**, correspondiente a la entrega, instalación, configuración y puesta en funcionamiento de los componentes que forman parte de la solución ofertada: 15 días calendarios, contados a partir del día siguiente de la suscripción del contrato.
- **Plazo de vigencia de licencia**: 730 días calendarios, contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal.

- **Plazo de la prestación accesoria**, **correspondiente al mantenimiento preventivo**: 730 días calendarios, contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal.

- **Plazo de la prestación accesoria**, **correspondiente al soporte técnico**: 730 días calendarios, contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal.

- **Plazo de la prestación accesoria, correspondiente a la capacitación**: 10 calendarios, contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal.

En concordancia con lo establecido en el expediente de contratación.

1.10. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar S/ 5.00 (Cinco con 00/100 Soles) en Caja de la Entidad y deberán recoger las bases en la Oficina de Licitaciones, para lo cual el participante debe adjuntar copia del comprobante de derecho de pago de reproducción de las bases y copia del mensaje confirmando la inscripción como participante en el procedimiento de selección impreso del SEACE.

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

1.11. BASE LEGAL

- Ley N° 28411, Ley Sistema Nacional de Presupuesto.
- Ley N° 31365, Ley de Presupuesto del Sector Publico para el Año Fiscal 2022.
- Ley N° 31366, Ley de Equilibrio Financiero del Presupuesto del Sector Publico para el Año Fiscal 2022.
- Ley N° 31367, Ley de Endeudamiento del Sector Público para el Año Fiscal 2022.
- Decreto Supremo N° 021-2019-JUS, TUO de la Ley Nº 27806, Ley de Transparencia y de Acceso a la Información Pública.
- Ley Nª 28015, Ley de Formalización y Promoción de la Pequeña y Microempresa. - Ley Nº 28411, Ley Sistema Nacional de Presupuesto. - Ley N° 29973, Ley General de Personas con Discapacidad.
- Decreto Supremo Nº 082-2019-EF, TUO de la Ley N° 30225, Ley de Contrataciones del Estado.
- Decreto Supremo Nº 168-2020-EF, Decreto Supremo que modifica el Decreto Supremo Nº 344-2018-EF del Reglamento de la Ley de Contrataciones del Estado.
- Decreto Supremo Nº 004-2019-JUS, TUO de la Ley N° 27444 – Ley del Procedimiento Administrativo General.
- Decreto Supremo N º 008-2008-TR, Reglamento de la Ley MYPE
- Decreto Legislativo Nº 1440, Decreto Legislativo del Sistema Nacional de Presupuesto Público.
- Decreto Supremo Nº 013-2013-PRODUCE - Texto Único Ordenado de la Ley de Impulso al Desarrollo Productivo y al Crecimiento Empresarial.
- Directivas, Pronunciamientos, y Opiniones del OSCE.
- Código Civil.
- Decreto Supremo N° 103-2020-EF, Decreto Supremo que establece disposiciones reglamentarias para la tramitación de procedimientos de selección que se reinicien en el marco del Texto único Ordenado de la Ley N° 30225.
- Decreto Supremo N° 020-2020-SA, Decreto Supremo que prorroga la Emergencia Sanitaria declarado por Decreto Supremo N° 008-2020-SA.

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

CAPÍTULO II
DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

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

2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos[2], la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

a) Declaración jurada de datos del postor. (**Anexo 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 – PIDE[3] y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir el certificado de vigencia de poder y/o documento nacional de identidad.

c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. **(Anexo N° 2)**

d) Declaración jurada de cumplimiento de las Especificaciones Técnicas contenidas en el numeral 3.1 del Capítulo III de la presente sección. (**Anexo N° 3**)

[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) Declaración jurada de plazo de entrega. **(Anexo Nº 4)**[4]

f) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio, así como el porcentaje equivalente a dichas obligaciones. **(Anexo Nº 5)**

g) El precio de la oferta en SOLES. Adjuntar obligatoriamente el **Anexo Nº 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.

h) Los componentes que forman parte de la solución ofertada deben cumplir todas las especificaciones técnicas requeridas en el numeral A 1.1; lo cual se debe acreditar fehacientemente para la presentación de la propuesta con información técnica complementaria pública y oficial del fabricante, tales como: catálogos y/o brochure y/o folletería y/o instructivos y/o fichas técnicas y/o manuales[5]

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

2.2.1.2. Documentos para acreditar los requisitos de calificación

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

2.2.2. Documentación de presentación facultativa

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

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

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

a) Garantía de fiel cumplimiento del contrato. CARTA FIANZA, que deberá señalar lo siguiente (Acorde con la Directiva Administrativa N° 001-2020/INEN/OGA-OCF):
   - El nombre o razón social del afianzado y N° de RUC. En caso de Consorcio deberá señalar de forma expresa el nombre completo o la denominación y la razón social de cada uno de los integrantes que conforman el consorcio.
   - El bien, servicio u obra a adquirirse o contratar, según corresponda y que es objeto de garantía.
   - Numero de procedimiento de selección.
   - Señalar el lugar de notificación en el caso de ejecución.

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,

[4] En caso de considerar como factor de evaluación la mejora del plazo de entrega, el plazo ofertado en dicho anexo servirá también para acreditar este factor.
[5] **En concordancia con la consulta presentada por la empresa Micro Solutions TI S.A**

de ser el caso.

d) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y la entidad bancaria en el exterior.
e) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
f) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.
g) Domicilio y correo electrónico para efectos de la notificación durante la ejecución del contrato.
h) Detalle de los precios unitarios del precio ofertado[6].
i) El Contratista deberá garantizarlo para la suscripción del contrato, con una declaración jurada donde se indiquen los datos de contacto.
j) Los documentos que acrediten el perfil señalado para el *Jefe de Proyectos y Coordinador en Seguridad* se presentarán como parte de la documentación para la suscripción del contrato, y corresponderán a lo siguiente: copia simple del título profesional. Asimismo, la experiencia deberá ser acreditada 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, las cuales serán presentadas como parte de la documentación para la suscripción del contrato. En cuanto, a las certificaciones, éstas deberán ser acreditadas con copia simple de constancia, certificados, u otros documentos según corresponda, las cuales serán presentadas como parte de la documentación para la suscripción del contrato.
k) *El personal especialista en seguridad*, se constituye como personal clave, y estará a cargo de la instalación, configuración y puesta en funcionamiento de la solución ofertada. Deberá presentarse la copia simple de su título profesional o técnico, como parte de la documentación para la suscripción del contrato. Asimismo, las certificaciones deberán ser acreditadas con copia simple de constancia, certificados, u otros documentos según corresponda, las cuales serán presentadas como parte de la documentación para la suscripción del contrato.
l) El proveedor debe estar certificado y/o acreditado por el fabricante de la marca de antivirus para comercializar los componentes que forman parte de la solución ofertada en el Perú; lo cual permite asegurar la procedencia legal acorde al cumplimiento de los procedimientos de garantia del fabricante en el Perú, y será acreditado con carta de la subsidiaria del fabricante en el Perú y/o carta del fabricante, la cual será presentada para la suscripción del contrato[7].

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE[8] 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).

Importante

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

- *En los contratos derivados de procedimientos de selección por relación de ítems, cuando el*

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

[7] **En concordancia con la consulta presentada por la empresa Micro Solutions TI S.A**

[8] 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/

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

Importante

- *Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.*
- *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya[9].*
- *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 Digital a través del enlace https://plataforma.inen.sld.pe/MesaPartesDigital/ a cargo de la Unidad de Tramite Documentario del Instituto Nacional de Enfermedades Neoplásicas, en el horario de 08:15 a 16:15 horas.

Nota: Los documentos presentados fuera de los horarios señalados se considerarán presentados a las 8:15 horas del día siguiente hábil.

Cuando se constituya garantía mediante carta fianza: Se presentará en Mesa de Partes ubicada en sito en la Av. Angamos Este N° 2520 - Surquillo, en el horario de 08:15 a 16:15 horas.

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 compra, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200,000.00).

2.5. FORMA DE PAGO

Pago por la prestación principal:
La Entidad realizará el pago de la contraprestación pactada a favor del contratista en PAGOS UNICO, 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 efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Recepción del Almacén General del INEN.
- Informe del funcionario responsable de la Oficina de Informática, previo informe de la Unidad Funcional de Servicios de Tecnología de Información y Comunicaciones, emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.

Pago por la prestación accesoria correspondiente al mantenimiento preventivo:

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

La Entidad realizará el pago del monto contratado por esta prestación en cuatro PAGOS PARCIALES, cada uno por igual monto; previa acta de conformidad.

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

- Informe del funcionario responsable de la Oficina de Informática, previo informe de la Unidad Funcional de Servicios de Tecnología de Información y Comunicaciones, emitiendo la conformidad de la prestación efectuada
- Comprobante de pago.

Pago por la prestación accesoria correspondiente a Capacitación

La Entidad realizará el pago del monto contratado por esta prestación en PAGO ÚNICO, previa acta de conformidad.

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

- Informe del funcionario responsable de la Oficina de Informática, emitiendo la conformidad de la prestación efectuada, por concepto de la capacitación.
- Comprobante de pago.

Dicha documentación se debe presentar en Mesa de Partes del Almacén General del Instituto Nacional de Enfermedades Neoplásicas, sito en Av. Angamos Este N° 2520, Distrito de Surquillo.

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. ESPECIFICACIONES TÉCNICAS

PERÚ | Sector Salud | Instituto Nacional de Enfermedades Neoplásicas | INEN

"DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES"
"AÑO DEL FORTALECIMIENTO DE LA SOBERNIA NACIONAL"

ESPECIFICACIÓN TÉCNICA N° 161-2022-OI-OGA/INEN	
DENOMINACIÓN	ADQUISICIÓN DE SOLUCIÓN DE PROTECCIÓN DE VIRUS INFORMATICOS
FINALIDAD PÚBLICA	Salvaguardar la información, y asegurar la operatividad y continuidad de los diversos servicios informáticos que brinda el INEN ante ataques de virus informáticos; contribuyendo así al cumplimiento de los objetivos establecidos por la Institución y permitiendo a sus dependencias el cumplimiento de las funciones señaladas en su reglamento de organización y funciones aprobado mediante D.S N° 001-2007-SA y sus modificatorias, buscando de esta manera elevar los niveles de eficiencia y satisfacción de los usuarios internos, pacientes y sociedad en general.
OBJETIVO	Gestionar la seguridad informática de la red del Instituto Nacional de Enfermedades neoplásicas ante ataques de virus informáticos como: gusanos, troyanos, phishing, adware, spyware; y así prevenir, mitigar y/o eliminar por el periodo de dos (02) años, todo tipo de software malicioso del parque informático del INEN (equipos de cómputo y servidores), compuesto por 1800 nodos.
CANTIDAD	Una solución de protección de virus informáticos para 1800 nodos.
ANTECEDENTES	El INEN como instituto especializado en el diagnóstico y tratamiento del cáncer, atiende todo el año a una masiva población que acude a diario; es por eso muy necesario que todos los servicios operen ininterrumpidamente; además que el equipamiento y personal trabajen como uno solo, ofreciendo un servicio de calidad y disponible. Por lo que uno de los objetivos es mantener los equipos informáticos y la red institucional protegida de virus y ataques maliciosos.
CÓDIGO SIGA MEF	140400031574
DEPARTAMENTO SOLICITANTE	INEN
ÁREA USUARIA	OFICINA DE INFORMÁTICA
A1	ESPECIFICACIONES TÉCNICAS REQUERIDAS
A1.1	PROTECCIÓN DE VIRUS INFORMÁTICOS

FUNCIONALIDAD ANTIVIRUS	
SOLUCIÓN DE ANTIVIRUS	El fabricante del producto deberá contar con representación local en Lima – Perú, quien deberá estar en condiciones de brindar servicio técnico en caso el Contratista no esté disponible.
	El producto debe ser del mismo fabricante en todos sus componentes.
	El producto deberá poder instalarse en sistemas operativos Linux, macOS y Windows tales como Windows Server 2012, Windows Server 2016, Windows Server 2019; y además; Windows 8, Windows 10 y Windows 11 con soporte para 32 y 64 bits.
	El producto debe estar en idioma español.
	El producto deberá incluir un motor de detección de malware basados en firmas del fabricante, asimismo, deberá incluir la inteligencia aplicada por el EDR.
	El producto debe incluir un sistema de análisis basado en algoritmos heurísticos capaces de detectar malware por similitud.
	El producto debe incluir tecnología basada en el análisis del comportamiento de amenazas logrando detenerlas incluso sin estar firmadas.
	El producto debe contar con un módulo de detección en tiempo real que proteja contra: virus, gusanos, troyanos, keyloggers, dialers, adware, spyware, hackools, rootkits, bots, herramientas de control remoto, y otros programas potencialmente peligrosos.
	El producto debe ser capaz de monitorear el comportamiento de aplicaciones específicas, para determinar el posible uso o intento de modificación de estas aplicaciones por agentes maliciosos y bloquear estas acciones.
	El producto debe ser capaz de revisar llaves específicas del registro del sistema operativo e impedir intentos de modificación, de escritura y de lectura.
	El producto debe ser capaz de evitar que sus procesos, servicios, archivos o archivos de registro puedan ser detenidos, deshabilitados, eliminados o modificados, para que de esta manera garantizar su funcionamiento ante cualquier tipo de ataque de virus.
	El producto debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

	carpeta especifica.
	El producto debe poder realizar escaneos manuales o programados, indicándose las unidades a escanear o las carpetas especificas que requieren ser escaneadas.
	El producto debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.
	El producto debe permitir habilitar notificaciones desde la interfaz del usuario, a fin de habilitar excepciones a políticas de restricción de aplicaciones, dispositivos y páginas web restringidas
	El producto debe contar con un cliente antivirus que le permita ser administrado desde una consola centralizada. La cual también podría alojarse en la nube siempre y cuando no se pierda ninguna funcionalidad ofertada en el producto base.
	El producto debe contar con un módulo de protección especialmente diseñado para hacerle frente a todo tipo de amenazas de tipo RANSOMWARE cual deberá permitir poner en cuarentena la amenaza y si fuese necesario incluir una lista blanca de aplicaciones especificamente para este módulo.
	El producto debe poseer un módulo avanzado de alerta temprana contra amenazas de reciente aparición que trabaje mediante la transmisión de información relacionada con las amenazas desde la nube.
	El producto debe contar con actualizaciones compactas e incrementales que eviten la generación de archivos de gran tamaño, evitando de esta manera que pueda impactar de una manera negativa a los recursos de ancho de banda de la red.
	El producto debe contar con un sistema de distribución de firmas a través de protocolo peer to peer a fin de optimizar en tiempo y recursos el proceso de distribución de firmas de virus informáticos a toda la red.
	Capacidad de generar dentro de la misma solución antivirus, repositorios de actualización, sin depender de aplicaciones externas.
	El producto debe tener la capacidad de establecerse en un modo silencioso, deshabilitando todas las notificaciones del mismo y evitar molestias al usuario.
	La solución ofertada deberá contar con un sistema avanzado de alerta que permite combatir con las amenazas emergentes según su reputación. Este sistema permitirá recopilar información anónima del ordenador afectado con las amenazas detectadas recientemente. Esta información podrá incluir una muestra o copia del archivo donde esté la amenaza, la ruta del archivo, el nombre del archivo, la fecha y la hora es información sobre el sistema operativo del ordenador.
	La protección de archivos en tiempo real contra malware debe tener las siguientes opciones: • Debe tener niveles predefinidos de protección e igualmente debe permitir al usuario personalizar el nivel de protección de acuerdo a sus requerimientos. • Debe permitir escanear archivos comprimidos. • Debe permitir la exclusión de unidades, carpetas o archivos a escanear por la protección en tiempo real. • Debe tener un motor heurístico para detección de posibles nuevos virus o basados en firmas.
	El producto debe contar con un módulo de protección en tiempo real para clientes de correo electrónico.
	El producto debe tener un módulo de protección en tiempo real para web: • El producto debe escanear y proteger contra archivos potencialmente maliciosos o escanear a través de protocolos o puertos. • Debe tener niveles predefinidos de protección e igualmente debe permitir al usuario personalizar el nivel de protección de acuerdo a sus requerimientos. • Debe ser capaz de escanear a través del protocolo SSL (HTTPS), de manera que se pueda impedir la descarga de archivos infectados. • Debe permitir realizar exclusiones de URL para que no sean analizadas por el antivirus tanto en el protocolo HTTP, FTP, HTTPS.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

	• Debe proteger contra phishing. • Debe tener un motor heurístico para detección de posibles nuevos virus.
	El producto debe tener un módulo de control de dispositivos: • Permite el acceso de solo lectura, lectura/escritura o bloquear dispositivos de acuerdo a una lista predefinida que incluya como mínimo: dispositivos USB, CD-ROM y dispositivos Bluetooth. • Debe tener la capacidad de permitir que tipos de dispositivos puedan ser utilizados en el entorno de la red.
	El producto debe tener un sistema de prevención de intrusos, este sistema debe encontrarse disponible para el host y debe proteger el sistema frente a un código maliciosos o cualquier actividad no deseada que intente perjudicar la seguridad del ordenador.
	Deberá tener una versión con soporte activo para equipos de baja performance sin afectar su rendimiento y funcionalidad.
	El producto debe incluir tecnologías de Machine Learning que le permitan automatizar el aprendizaje de nuevas amenazas de malware a través de sus diferentes sensores o tecnologías propuestas.
	El producto debe contar con tecnología de inteligencia artificial y aprendizaje automático capaz de reconocer y actuar sobre ataques de tipo malware ofuscado.
CONSOLA DE ADMINISTRACIÓN CENTRALIZADA	La consola de administración podrá instalarse en la nube o en sistemas operativos tales como Windows Server 2012, Windows Server 2016, Windows Server 2019; y además, Windows 8, Windows 10 y Windows 11 con soporte para 32 y 64 bits.
	La consola de administración deberá integrar un sistema de autenticación basado en Windows para el acceso a la consola de administración.
	La consola de administración deberá ser de tipo On-Premise permitiendo instalarse en los servidores del INEN, o puede gestionarse desde la nube; en este caso se deberá utilizar alguna herramienta y/o tecnología que permita la conexión segura a la consola.
	La consola de administración debe estar en idioma español.
	La consola de administración deberá poder lanzar tareas de instalación, despliegue y desinstalación de clientes en forma remota.
	La consola de administración deberá poder mandar mensajes a clientes individuales o a grupos de clientes e informar a los usuarios de forma rápida y sencilla las acciones que se van a tomar.
	La consola de administración debe tener la capacidad de desinstalar remotamente cualquier solución antivirus que se encuentre implementada en las estaciones de trabajo y servidores, sin la necesidad de la contraseña de remoción del actual antivirus.
	La consola de administración debe permitir la configuración y administración remota de la solución antivirus instalada en las estaciones de trabajo y servidores (Windows y Linux).
	La consola de administración deberá poder mostrar un resumen de la instalación indicando el estado y sugiriendo una acción de refuerzo si fuese necesario.
	La consola de administración deberá poder gobernar todos los antivirus residentes en las diferentes plataformas que tenga la institución Windows, Linux, Mac, Android, iOS y plataformas de virtualización como VMWare y Microsoft HyperV.
	La consola deberá ser 100% web permitiendo implementar una nube privada a través de un componente web seguro (https), a fin de poder gestionar estaciones de trabajo o Laptops que se encuentren fuera de la red corporativa de forma transparente.
	La consola de administración deberá poder registrar eventos creando logs por cada uno de los eventos que realice dependiendo del ítem (exploración, actualización, bloqueos, etc.)
	La consola de administración deberá permitir implementar exclusiones en la exploración, con capacidad para excluir de la exploración archivos, directorios y/o procesos, etc.; de forma centralizada.
	La consola de administración deberá permitir definir a través del residente acciones posteriores a la detección, capacidad para tomar distintas acciones cuando sea detectado un virus, o un

	ataque, limpiar el archivo infectado, moverlo a cuarenta, continuar la exploración, no tomar acción, eliminar el archivo, etc.
	La consola de administración deberá permitir también definir acciones posteriores a la detección para una exploración bajo demanda, capacidad para tomar distintas acciones cuando sea detectado el virus, ataque o programa no deseado: limpiar el archivo infectado, moverlo a cuarentena, continuar la exploración, no tomar acción, eliminar el archivo, etc.
	La consola de administración deberá permitir definir la exploración de correo electrónico con capacidad para exploración de mensajes de correo electrónico utilizando Microsoft Outlook, detención de virus y programas no deseados.
	La consola de administración deberá permitir la programación de tareas, capacidad para programar tareas de exploración, actualización, etc.
	La consola de administración deberá permitir la configuración de repositorios para actualización, capacidad para agregar/eliminar repositorios hacia donde se descarga la actualización de las definiciones de virus.
	La consola de administración deberá permitir que la distribución de firmas de malware también pueda darse de forma peer to peer, esto para simplificar, acelerar y optimizar el proceso de distribución de firmas en una red corporativa para de esta manera tener en el menor tiempo posible a todos los equipos actualizadas y en condiciones de hacerle frente al malware.
	La consola de administración deberá mostrar un inventario general de todos los equipos protegidos en la red logrando especificar el hardware y software que tienen instalado todos y cada uno de los nodos protegidos (estaciones de trabajo y servidores).
	La consola de administración deberá contar mínimamente con dos tipos de autenticación para loguearse en el servidor antivirus, el primero deberá trabajar con las credenciales de Windows y el segundo con un usuario integrado previamente configurado en la consola
	La consola de administración debe permitir la creación de distintos usuarios para acceder a la consola, asignar distintos permisos y roles según lo asignado al usuario.
	La consola de administración deberá poder programar análisis de malware en todos los equipos y servidores de la red sin que esto implique una saturación del procesador o memoria para realizar esta actividad, para esto se deberá poder especificar que el escaneo se realice utilizando los tiempos muertos del usuario, el objetivo es evitar saturar los recursos cuando el usuario los necesite.
	La consola de administración deberá contar con una cuarentena local capaz de aislar posibles amenazas de malware no firmadas, pudiendo liberar y limpiar programas y/o aplicaciones según convenga el administrador.
	La consola de administración deberá poder reportar y enviar directamente al fabricante, software y/o amenazas no firmadas para su evaluación.
	La consola de administración deberá poder integrarse con el directorio activo a fin de llevar una sola gestión (grupos organizativos).
	La consola de administración deberá poder definir intervalos de sincronización con clientes y servidores de subred, a fin de que el administrador determine la mejor configuración entorno a su red.
	La consola de administración deberá permitir configurar alertas que podrán ser enviadas de forma automática a un determinado correo electrónico.
	La consola de administración deberá permitir lanzar tareas de UPGRADE de versión de clientes de forma automática y/o programada.
	La consola de administración deberá tener la capacidad de definir políticas de bloqueo de configuraciones por medio de una contraseña. Este bloqueo debe ser selectivo para configuraciones de objetos específicos.
	La consola de administración deberá poder aplicar configuraciones a equipos con bajo performance a fin de que tengan la capacidad de adaptarse a los recursos disponibles por el usuario, se deberá poder habilitar un solo motor de firmas en caso de proteger equipos con muy bajo performance (Por ejemplo, equipos con procesador 2 CPU y 1 GB RAM

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

	La consola de administración deberá estar desarrollada sobre una arquitectura multitenant a fin de poder implementar de forma transparente nuevos escenarios de protección en diferentes redes a nivel nacional en el tiempo, integrando la gestión de diferentes consolas con sus propios recursos y condiciones en una sola.
	La consola de administración deberá poder programar despliegues de nuevas versiones de antivirus (Archivos de programas).
	Este sistema deberá tener la capacidad de generar reportes locales en cada equipo referentes a todas las transacciones realizadas por cada producto.
	La consola de administración deberá permitir generar reportes individuales y personalizados, relacionados a equipos y archivos afectados.
	La consola de administración deberá permitir bloquear puertos de comunicación para combatir epidemias. Así como también crear políticas de denegación de escritura en forma centralizada para evitar epidemias.
	La consola de administración tendrá la capacidad de hacer un "trace" de los equipos de red que se encuentren infectados y tendrá la capacidad de bloquear este equipo remotamente no permitiéndoles mayor comunicación con la red.
	El producto debe permitir al administrador visualizar características de la PC, y filtrarlas respectivamente, tales como Sistema Operativo, Nombre de la PC y dirección IP, Dominio al que pertenece, Memoria Disponible, BIOS, Versión del BIOS, Nombre del Sistema, Versión del Sistema, Softwares Instalados y Su Respectiva Fecha de Instalación.
	El producto debe poseer una interfaz web que permita monitorear el estado de los equipos en la red, así como también una gama de múltiples reportes como el estado de carga de servidor, clientes con más amenazas, clientes actualizados y no actualizados.
	La consola de administración debe permitir la generación de reportes gráficos y personalización de los mismos.
	La consola deberá incluir un sistema de análisis de vulnerabilidades derivadas de plataformas Windows y programas de terceros que permita la descarga centralizada de parches, la aplicabilidad, la distribución y la instalación remota de estos. Este sistema debe estar integrado al software antimalware por lo que no deberá requerir la instalación de ningún componente adicional para su normal desempeño.
	La consola deberá poder lanzar pruebas de aplicabilidad de parches a fin de evitar errores del sistema como producto de la instalación remota de parches que deriven de programas instalados y la misma plataforma.
	El licenciamiento debe incluir un sistema de gestión y distribución de parches que permita el análisis de vulnerabilidades derivadas de plataformas Windows y programas de terceros que permita la descarga centralizada de parches, la aplicabilidad, la distribución y la instalación remota de estos.
ATRIBUTOS DE PREVENCIÓN	Se debe contar con un módulo de control de aplicaciones que permita implementar políticas de seguridad que conlleven a definir aplicaciones en lista negra para evitar que estas se ejecuten en las estaciones de trabajo y servidores de la red; reconociendo el hash, versiones y fabricantes específicos de las aplicaciones a bloquear.
	El módulo de control de aplicaciones debe permitir la implementación de políticas de seguridad para el control de aplicaciones el mismo que deberá poder definir aplicaciones en lista blanca que permitan que solo estas puedan ejecutarse en determinadas estaciones de trabajo y servidores de la red.
	El módulo de control de aplicaciones deberá poder aplicar políticas de seguridad a directorios y archivos específicos.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

	El módulo de control de aplicaciones deberá permitir que el usuario pueda solicitar permiso de acceso a determinada aplicación bloqueada desde su PC a fin de mejorar los tiempos de respuesta con el usuario.
	Deberá incluir una protección contra dispositivos USB físicos manipulados.
	Deberá tener un módulo que permita la implementación de políticas de seguridad para el control de dispositivos extraíbles, el mismo que deberá poder ser desplegado, habilitado o deshabilitado desde la consola de administración.
	El módulo de control de dispositivos deberá tener la capacidad de asignar privilegios de solo lectura a cualquier USB de almacenamiento externo que se conecte al equipo a fin de evitar que cualquier aplicación de peligro se escriba o ejecute desde este medio.
	El módulo de control de dispositivos deberá permitir que el usuario pueda solicitar permiso de acceso a su dispositivo desde su PC a fin de mejorar los tiempos de respuesta con el usuario.
	El módulo de control de dispositivos deberá permitir la creación de listas blancas específicas construidas a partir del reconocimiento del ID del hardware de cada USB de almacenamiento.
	Deberá tener un módulo que permita la implementación de políticas de seguridad para la navegación web el mismo que no debe necesitar instalar ningún tipo de plugin o componente adicional para escanear y filtrar contenido en los navegadores (Browsers soportados, Internet Explorer, Firefox y Chrome).
	El módulo de filtro web debe proveer al administrador la facultad de definir filtros en base a categorías para la navegación de los usuarios finales conectados o desconectados de la red. Estas categorías deben comprender sexo, pornografía, navegadores anónimos, desnudos, redes sociales, música, videos y otros. Además, debe permitir ingresar páginas web específicas para permitir como excepción o bloquear adicionalmente.
	El módulo de acceso a internet deberá permitir definir días, horas de acceso a internet para determinados grupos o PCs en particular.
	Deberá incluir un módulo que proteja las transacciones bancarias sin necesidad de implementar plugins ni componentes adicionales.
	Deberá incluir un módulo de monitoreo de redes que permita monitorear la red permitiendo la creación y análisis de métricas de evaluación para discos duros, servicios críticos, CPUs, impresoras, enrutadores, switches, servidores web, servidores de correo y servidores de base de datos a fin de establecer semáforos que faciliten la lectura de informes y alertas de anomalías presentadas en la red, a fin de detectar oportunamente tendencias de rendimiento.
	Deberá permitir implementar tareas de escaneo de malware en modo de reposo para de esta forma evitar saturar los recursos de los equipos.
	El escaneo en modo de reposo permitirá definir carpetas y/o directorios específicos para su análisis.
	Deberá contar con módulo de protección que permita auditar la seguridad a nivel físico de cualquier dispositivo USB que se conecte al equipo asegurándose de que de este no este corrupto con algún tipo de keylogger físico, el sistema deberá solicitar un código de seguridad cada que se conecte un nuevo dispositivo.
ATRIBUTOS DE MITIGACIÓN	Deberá mitigar el daño provocado por contagios; cierra los puertos, monitorea aplicaciones y motores de correo electrónico, analice archivos y carpetas, que efectúe seguimientos y bloquee las comunicaciones que generen una infección.
	Deberá incluir protección que amenace específicamente las vulnerabilidades del sistema operativo, deberá incluir protección anti-exploit capaz de proteger de esas amenazas que aprovechan las brechas de seguridad en los programas instalados, desde editores de texto hasta plugins de los navegadores.
	Deberá contar con un módulo de gestión de parches centralizado capaz de reconocer vulnerabilidades que derivan de la ausencia de parches en el sistema operativo y programas instalados en PCs/Servidores.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

	El módulo de gestión de parches deberá ser capaz de clasificar los parches que necesitan aplicarse en las estaciones de trabajo y servidores a fin de cerrar los huecos de seguridad encontrados, así como lanzar pruebas de aplicabilidad de los mismos a fin de asegurarse de que estos no ocasionen problemas de compatibilidad.
	El módulo de gestión de parches deberá ser capaz de realizar tareas de rollback (desinstalación remota de parches desde consola) en caso de requerirse.
	Deberá contar con un cortafuego administrable capaz de monitorear todo el tráfico entrante y saliente en todas y cada una de las PCs de la red.
	El cortafuego deberá poder ser implementado en modo de piloto automático reconociendo todo el tráfico para luego implementar reglas específicas.
	El cortafuego deberá poder notificar cuando una aplicación sea bloqueada.
	El cortafuego deberá tener un asistente de configuración que permita implementar reglas de restricción y permiso a determinadas aplicaciones y puertos.
	Si el administrador así lo prefiere se podrá habilitar opción de desactivar cortafuego desde el cliente.
ATRIBUTOS DE DETECCIÓN	Deberá incluir tecnología innovadora para PC y Servidores que detenga y elimine proactivamente el software malicioso, extienda la cobertura contra nuevos riesgos de seguridad y reduzca el costo de respuesta frente a epidemias.
	Deberá permitir defender los sistemas contra virus, gusanos, troyanos, phishing, adware y spyware.
	Deberá bloquear las amenazas que no escriben en el disco duro con el escaneo en memoria.
	Deberá contar con un módulo de protección contra Botnets, este módulo debe ser capaz de detectar conexión con servidores maliciosos de comando y detectar patrones típicos de equipos que forman parte de una Botnet.
	Deberá contar con protección contra ransomware que supervise el comportamiento de las aplicaciones y los procesos que intentan modificar los datos.
	Deberá bloquear una amplia gama de virus y amenazas de código malicioso, incluso los que están ocultos en archivos comprimidos; que descubra virus desconocidos con detección heurística y genérica.
	Deberá proteger contra exploits dirigidos a aplicaciones y servicios Microsoft, especialmente a servicios del sistema operativo Microsoft Windows, Microsoft Word, Microsoft Excel, Microsoft Outlook.
	Deberá incluir un antivirus residente capaz de analizar diferentes protocolos de comunicación como HTTP, HTTPS, SMPT, POP, IMAP y otros.
	El residente antivirus deberá poder tomar diversas acciones en caso de una infección, bloquear el acceso al archivo, desinfectar y copiar en cuarentena para su análisis, mandar a cuarentena o eliminar el archivo.
	El residente antivirus deberá poder tomar diversas acciones en caso de analizar archivos comprimidos, bloquear el acceso al archivo, desinfectar y copiar en cuarentena para su análisis, mandar a cuarentena o eliminar el archivo.
	El residente de antivirus deberá poder configurarse en acceso a lectura, escritura y al ejecutar para que se esta manera se tenga mejor visibilidad de todos los archivos que se escriban en disco.
	El residente de antivirus deberá poder comprobar la existencia de virus informáticos en correos recibidos / enviados en el cliente de correo. Adicionalmente se podrá realizar la comprobación solo en los correos no leídos.
	El residente de antivirus deberá poder adjuntar un informe de ante un correo electrónico infectado.
	El residente deberá detectar y neutralizar amenazas de los programas maliciosos en los correos masivos antes incluso de que estén disponibles las actualizaciones de las firmas de virus correspondientes.

ATRIBUTOS DE RECUPERACIÓN	Deberá permitir crear un CD, DVD o USB de arranque para efectuar un análisis completo de un equipo o servidor, este análisis se debe realizar antes de que arranque el sistema operativo instalado y utilizar firmas de virus actualizadas, esto a fin de recuperar un sistema infectado.
	Deberá contar con un módulo de copias de seguridad de información sensible que permita programar y ejecutar copias de seguridad de los archivos y carpetas más críticas en los clientes de forma diferencial y automática.
	El módulo de copias de seguridad debe escanear la data respaldada garantizando de esta manera de que se resguarden copias sin virus.
	El módulo de copias de seguridad debe permitir definir el destino de la información a respaldar, así como programar la tarea para determinado día con determinada frecuencia.
	El módulo de copias de seguridad debe permitir programar tareas de copias completas y parciales.
	El módulo de copias de seguridad debe permitir considerar exclusiones basado en extensiones, esto a fin de evitar respaldar música, videos y/o archivos de ocio del usuario.
TECNOLOGÍA EDR	La gestión centralizada del EDR puede estar integrada en la consola de la solución Antivirus o puede tener su propia consola ya sea en modalidad On-Premise o en la Nube; y que pueda instalarse en sistemas operativos tales como Windows Server 2008, Windows Server 2008 (R2), Windows Server 2012, Windows Server 2016, Windows Server 2019; y además; Windows 7, Windows 8, Windows 10 y Windows 11 con soporte para 32 y 64 bits.
	La solución EDR debe estar instalada en los 1800 equipos informáticos donde se tiene implementada la solución Antivirus; por lo cual podrá ser instalado en los sistemas operativos tales como Windows Server 2008, Windows Server 2008 (R2), Windows Server 2012, Windows Server 2016, Windows Server 2019; y además; Windows 7, Windows 8, Windows 10 y Windows 11 con soporte para 32 y 64 bits.
	La solución debe ser capaz de detectar malwares Zero-Day y APT y las tres etapas del ciclo de vida de ataque de malware moderno: Exploit, Dropper y Data Exfiltration.
	El fabricante de la solución debe poseer servicios de detección y respuesta gestionada en el cual permita el acceso a la información de incidentes a través de un portal web.
	La solución debe proporcionar detección en tiempo real del malware desconocido.
	La solución de protección debe poder tomar entradas para indicadores personalizados de compromiso.
	La solución debe proporcionar información sobre la actividad de los sistemas y resultados analíticos, que incluyen: actividad y estado del sistema, longitudes de cola, eventos registrados, su estado y las tecnologías utilizadas para proporcionar veredictos, listas de IP, dominios y correos electrónicos más frecuentemente relacionado con incidentes.
	La solución debe tener la capacidad de incluir una lista negra en la nube.
	La solución debe proporcionar una visibilidad completa con sus capacidades forenses, monitoreo y registro de eventos de puntos finales, archivos afectados, procesos iniciados, cambios en el registro del sistema y actividad de la red.
	La función de investigación debe incluir datos históricos de todos los eventos de puntos finales primarios para determinar tanto los cambios técnicos que se produjeron como el efecto comercial.
	La solución debe tener diferentes funciones de administrador que tengan una única interfaz/ panel durante el inicio de sesión y controladas por privilegios y funciones (Administrador, Revisor, investigador, etc.).
	La extracción del archivo debe escanearse utilizando el laboratorio de virus interno, sin enviar muestra fuera de la red.
	Los datos forenses deben ser en tiempo real y exhaustivos, mostrando el nivel de compromiso y permitiendo a los administradores tomar decisiones; asimismo, esos datos deben almacenarse en el local dentro de la plataforma.
	La solución debe detectar malware avanzado de día cero que las soluciones basadas en firmas

	normalmente no detectan.
	La solución debe poder analizar cualquier tipo de archivo mediante el uso de múltiples aplicaciones y múltiples versiones, que incluyen, entre otros: exe, dll, pdf, doc, docx, xls, xlsx, gif, jpeg, png, tiff, swf, mov, qt, mp4, jpg, mp3, asf, ico, htm, url, rm, com, vcf, ppt, rtf, chm, hlp y otros.
	La solución debe ser capaz de identificar con precisión el malware y mantener una tasa de falsos positivos muy baja. La detección debe incluir protección contra malware omitido por productos de seguridad existentes.
	La solución debe poder enviar notificaciones al correo electrónico sobre los incidentes que se van presentando.
	La solución debería ser capaz de lidiar con las técnicas de evasión de VM.
	La solución debe ser capaz de detectar ataques localmente, sin depender de un servicio en la nube.
	La solución debe tener la capacidad de aislar los equipos de la entidad que pueden resultar con amenazas, ello utilizando un aislamiento y recuperación del equipo a demanda del administrador.
	La solución debe contar con la capacidad de identificar cualquier indicador de compromiso a lo largo de la red y poder bloquearlo remotamente.
	La solución debe ser capaz de identificar con precisión los archivos maliciosos, que incluyen, entre otros, cualquier extensión de archivo, archivo u ofuscación.
	La solución debe tener la capacidad de verificar / ejecutar un análisis en todos los hosts para cualquier nombre de archivo, extensión de archivo, archivo MD5/SHA256 o IOC provisto.
	La solución deberá contar con sistemas backend automatizados o procesos de análisis automáticos y manuales capaces de identificar muchos Indicadores de Compromiso (IOC). Un IOC podría ser un servidor de comando y control (C&C) utilizado para operar una botnet, o un archivo en particular que ha sido identificado como malicioso.
	La solución debe tener la técnica Sandboxing que permite examinar aplicaciones en un ambiente controlado con el fin de determinar si es una aplicación confiable o no; y, además, en caso se trate de un programa malicioso, este pueda expandirse por toda la red.
	La solución debe defenderse contra ataques avanzados persistentes / de día cero, que incluyen, pero no se limitan a: • Malware en general. • Ataques de día cero. • Explotar la vulnerabilidad de software existente. • Ransomware. • Inyección SQL. • Hacktivismo. • Clickjacking. • Spyware. • Amenazas persistentes avanzadas / ataques dirigidos. • Ataques de botnet. • Rootkits. • Amenazas polimórficas. • Amenazas combinadas. • Malware ofuscado, malware desconocido y ataques de día cero. • Scripts maliciosos que aprovechan: PowerShell, Visual Basic, Perl, Python, Java /JAR. • Ataques residentes en la memoria y otros ataques sin malware. • Ataques basados en documentos (archivos PDF y macros). • Ataques de inicio de sesión remoto y el uso malicioso de software legítimo.

	• Malware conocido y variantes que incluyen ransomware basado en malware. Esto a través de una tecnología de detección basada en el comportamiento, que sea capaz de monitorear el comportamiento de aplicaciones almacenando cada acción observada en una base de datos gráfica local y ligera, identificando al propio malware por su comportamiento malicioso y no necesariamente por su firma.
FUNCIONALIDAD GESTIÓN DE ACTIVOS	
CARACTERÍSTICAS	Deberá incluir la funcionalidad de administración centralizada de incidentes, problemas y solicitudes de cambio de usuario final mediante un entorno web.
	Deberá integrar funcionalidades de gestión de inventario de activos de TI descubriendo y manteniendo el inventario de activos de TI con un descubrimiento automático.
	Deberá poder descubrir activos de TI de Windows, Linux, Mac, AIX y Solaris, así como impresoras, routers, switches y más.
	Deberá permitir descubrir, rastrear y administrar los activos de hardware y software de TI en un solo lugar.
	Deberá optimizar la utilización de los activos, evitando las vulnerabilidades y garantizando el cumplimiento de las licencias.
	Deberá permitir programar auditorías y escaneos periódicos de la red para estar siempre actualizado ante cualquier cambio en el entorno de TI.
	Deberá poder notificar a los técnicos ante cualquier cambio en los activos de TI durante el escaneo de red / dominio.
	Deberá poder programar un re escaneo automático de la red para descubrir nuevos equipos añadidos.
	Deberá poder habilitar "limpiezas de historial de escaneo" periódicos para reducir el desorden en la información.
	Deberá permitir realizar inventario de los activos, tanto de hardware como software.
	Deberá poder escanear los equipos que se encuentran dispersos por diferentes sitios para descubrir e importar todo el software instalado, automáticamente.
	Deberá presentar una única vista de cada software, capturando detalles críticos tales como, los equipos que están ejecutando el software, y el perfil del fabricante del software.
	Deberá poder clasificar el software como administrado, shareware, freeware, prohibido, y categorizarlo para un seguimiento y una gestión eficiente.
	Deberá permitir obtener un completo historial sobre cuándo un software fue instalado o desinstalado, usuarios anteriores del software, y los equipos donde se ejecutó.
	Deberá permitir realizar conexiones remotas de los técnicos a los equipos afectados por alguna incidencia.
	Deberá ser compatible con los procesos y prácticas de ITIL en la gestión de incidentes, problemas y requerimientos de cambios.
	Deberá poseer una aplicación móvil para dispositivos Android la cual debe estar disponible desde la playstore.
	Deberá permitir crear códigos de barra para los activos registrados.
	Debe permitir relacionar los activos a un departamento y usuario, así como también debe permitir elegir si el activo es propio o arrendado.
	Deberá permitir exportar informes en html, pdf, xls, xlsx y csv.
	Deberá permitir construir su propio catálogo de productos de TI y categorizar los productos basados en tipos y subtipos.
	Deberá integrase al directorio activo.
	Deberá poder integrarse a aplicaciones de gestión de vulnerabilidades, auditoria de directorio activo y mesa de ayuda.
FUNCIONALIDAD ANTISPAM	
CARACTERÍSTICAS	La solución deberá estar instalado y configurado localmente o en la nube cumpliendo los

	requisitos mínimos de privacidad de la información o GDPR.
	Deberá proteger un total de 2000 buzones en tiempo real.
	Deberá proteger el correo entrante y saliente
	Deberá analizar protocolos de e-mail de transferencia tipo SMTP y/o a nivel POP3, POP3S, IMP, IMAPS, IMAP4.
	Deberá contar con un sistema de administración seguro vía web (HTTPS). Desde el sistema de administración se deberá tener acceso a la creación de políticas entrantes y salientes, listas blancas y negras personales y globales, reportes, sistema de solicitud de reporte, cuarentenas, etc.
	Dashboard para estadísticas y reportes
	Deberá permitir aplicar filtros por usuario (listas blancas o negras de forma manual y/o automática), dominio, tipo de contenido, etc.
	Deberá poder detectar, eliminar y limpiar virus y spyware en los archivos adjuntos al correo electrónico y en el cuerpo del mensaje
	Deberá ofrecer un sistema de protección antispam en tiempo real con filtros.
	Deberá contar con un módulo para el filtrado por reputación que permita el bloqueo por IP's de servidores dudosos y permitir elaborar excepciones tanto a nivel MTA como a nivel de políticas de correo
	La solución debe estar en la capacidad de proteger contra virus informáticos ofreciendo por lo menos doble análisis de malware con diferentes tecnologías anti-virus a todo el correo entrante y saliente.
	El motor del anti-virus debe actualizarse de forma automática asegurando así la menor gestión y la máxima protección.
	Con respecto a la tecnología antispam esta debe presentar múltiples capas de análisis que permita asegurar los más altos niveles continuos de correo no deseado, estas capas deben incluir tecnologías de análisis tales como Sender Policy Framework, comprobación de destinatarios, SURBL, análisis bayesiano, palabra clave, un cabezazo de RBL y análisis del texto principal, los algoritmos de puntuación personalizadas, así como muchas otras reglas personalizadas. La solución debe poseer un módulo de filtrado de contenido que permita bloquear los archivos adjuntos no deseados incluyendo los tipos de archivos, tipos mime y archivos renombrados. Esto puede ser activado en el dominio y nivel de usuario que permite a los administradores bloquear los contenidos no deseados de acuerdo con la política de correo electrónico en la organización.
	La solución debe permitir llevar la gestión diaria del spam a los usuarios finales. Los usuarios finales deben tener una visibilidad completa de todo el correo bloqueado por la solución a fin de que a partir de su bandeja de entrada del usuario final tengan la capacidad de liberar cualquier correo electrónico requerido sin tener que recurrir al administrador de la solución.
	La solución debe proveer un conjunto de informes integrales que proporcionen información a través de gráficos automatizados como principales receptores de spam de correo electrónico, los destinatarios principales y todos los necesarios para identificar posibles amenazas de spammers. También debe tener un "reportador" de todo el correo a su paso por la solución a fin de generar estadísticas con capacidad de búsqueda.
	La solución debe tener un módulo de sandboxing capaz de proteger contra sofisticados ataques de correo electrónico al proporcionar un entorno para ejecutar análisis profundos y sofisticados de programas y archivos desconocidos o sospechosos.
	La capa de seguridad avanzada de sandboxing de correo electrónico proporcionará protección contra malware, phishing, amenazas persistentes avanzadas (APT), ofreciendo información sobre nuevas amenazas y ayudando a mitigar los riesgos.
	La solución debe permitir imprimir un mensaje personalizado que certifique el análisis del correo en calidad de aviso legal.
	La solución debe poder ser configurado para aceptar correo electrónico para un número ilimitado

		de dominios que a su vez se pueden transmitir a un número ilimitado de servidores de correo electrónico.
		La solución debe poder definir todas las reglas a fin de que estas se puedan establecer a cualquier dominio y a cualquier usuario. Esto permite una configuración detallada para todas las necesidades de la institución.
		Todas las actualizaciones, incluyendo antivirus, antispam, lanzamiento de nuevas versiones, la configuración de copia de seguridad, la espalda bayesiano y los informes de gestión deben generarse de forma automatizada.
		La solución debe contar con listas blancas y listas negras que se puedan configurar para el usuario o en un nivel de dominio y permitir / bloquear por dirección de correo electrónico completo o dominio.
		La solución debe proporcionar tanto el por el lado del administrador como por el usuario final una funcionalidad de búsqueda y recuperación de su correo electrónico enviado a cuarentena.
		La solución, en caso lo requiera, debe contener un conjunto completo de pruebas de diagnóstico e informes que proporcionen tanto el administrador y el fabricante toda la información necesaria para investigar a fondo los problemas de compatibilidad. Esto incluye la posibilidad de enviar un informe de diagnóstico por el fabricante vía remota SSH registro autenticado desde el mismo fabricante.
		Se debe poder acceder a todas las características de la solución mediante una interfaz intuitiva basada en la web. Esto permite el acceso controlado a partir de la red y elimina la necesidad de software de gestión basado en cliente.
		La solución debe poder limitar esta interfaz a personas y lugares desde donde se puede tener acceso.
		La solución, en caso lo requiera, debe presentarse como ISO o VMware que contenga la aplicación y debe tener su propio sistema operativo sobre una plataforma Linux endurecido, incluyendo secuencias de comandos para la instalación, por lo que no debería haber requisitos de ningún sistema operativo a fin de evitar sobrecostos.
		La solución debe incluir actualizaciones de versiones incluidas durante el tiempo de compra sin costo adicional.
		La licencia debe cubrir los 2000 buzones destinados a proteger.
		La solución debe certificar una eficacia mínima de detección de spam de 99,9%.
		La solución debe presentar mínimamente las siguientes opciones de informes: • Información del sistema: proporciona una descripción general del estado de la solución. • Gráficos: muestre estadísticas diarias, semanales y mensuales sobre la cantidad de correos electrónicos procesados, correos electrónicos marcados como spam o que contienen virus; en caso de soluciones locales, agregar las estadísticas sobre el uso de CPU, uso de memoria y uso de HDD. • Administración: proporciona una descripción general de los eventos administrativos durante los últimos treinta días. • Historial: Un registro de todo el correo que es procesado por el sistema. • Informes: Le debe permitir generar varios informes bajo demanda. • Programación de informes: le debe permitir programar informes diarios, semanales o mensuales que se pueden enviar por correo electrónico a una dirección de correo electrónico específica o a varias direcciones de correo electrónico. • Informes archivados: muestra todos los informes que se han archivado en Informes de hoy o Informes programados, en el caso de que la solución sea local.
A1.2	ALCANCES Y DESCRIPCIÓN DE LA ADQUISICIÓN	

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

	El Contratista deberá realizar la instalación, configuración y puesta en funcionamiento de la solución ofertada en los equipos informáticos del INEN, acorde a las especificaciones técnicas solicitadas, el cual debe contemplar como mínimo: • Instalación y configuración en todos los equipos de escritorio, portátiles y servidores del INEN • Instalación y configuración de la consola de administración local y remota. • Puesta en funcionamiento de la solución ofertada. • Pruebas de funcionamiento acorde a las especificaciones técnicas solicitadas.
A2	**CONSIDERACIONES**
	• Los componentes que forman parte de la solución ofertada deben cumplir todas las especificaciones técnicas requeridas en el numeral A 1.1, lo cual debe acreditar fehacientemente para la presentación de la propuesta con información técnica complementaria publica y oficial del fabricante tales como: catálogos y/o brochure y/o folleteria y/o instructivos y/o fichas técnicas y/o manuales y/o links del fabricante (portal web) y/o capturas de pantalla de la consola de administración de la solución ofertada.[1] • La funcionalidad antispam ofertada debe ser 100% compatible con la consola de gestión del Antispam de propiedad del INEN, lo cual garantizará su interoperabilidad. • El contratista debe incluir todos los accesorios, componentes y/o servicios necesarios, para el correcto funcionamiento y puesta en producción de la solución ofertada. El INEN no reconocerá pago adicional para este fin.
A3	**GARANTÍA COMERCIAL**
	La garantía debe ser brindada directamente por el fabricante y/o subsidiaria del fabricante en Perú para todos los componentes solicitados, el cual se contabilizará a partir de la fecha en que se otorga el Acta de Conformidad del bien por parte del área usuaria. • Los componentes que forman parte de la solución ofertada deben contar con 730 días calendario de garantía, contados a partir de la fecha en que se otorga el Acta de Conformidad del bien por parte del área usuaria. • La garantía debe incluir parches y actualizaciones a últimas versiones estables y liberadas por el fabricante. • La garantía debe incluir asistencia técnica como segunda instancia, ante incidentes que puedan manifestarse. Los alcances solicitados por la garantía comercial deben ser respaldados y garantizados por el fabricante de los componentes que forman parte de la solución ofertada.
A4	**SISTEMA DE CONTRATACIÓN Y MODALIDAD DE EJECUCIÓN**
	Suma alzada y llave en mano
A5	**PRESTACIONES ACCESORIAS A LA PRESTACIÓN PRINCIPAL**
A5.1	**MANTENIMIENTO PREVENTIVO**
	Las actividades de mantenimiento preventivo deberán ser realizadas por el Contratista, por un plazo de 730 días calendario, el cual debe incluir: Se deben realizar 4 mantenimientos. Cada mantenimiento se realizará dentro de un periodo no mayor a 30 días calendario. Las actividades correspondientes para el servicio de mantenimiento se iniciarán a partir del día calendario siguiente de haberse otorgado la conformidad por la prestación principal. Los mantenimientos se realizarán de acuerdo con el siguiente detalle:

N° de mantenimiento	Periodo dentro del cual se debe dar el mantenimiento	
	Inicio (a partir de)	Fin (plazo máximo para efectuar el mantenimiento)
1	153 días calendario	182 días calendario
2	336 días calendario	365 días calendario
3	518 días calendario	547 días calendario
4	701 días calendario	730 días calendario

[1] Se modificó el literal A2 de acuerdo a la consulta presentada por la empresa Micro Solutions TI S.A

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima - 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

	Nota: Tanto el inicio como el fin indicado en este cuadro, corresponden a los días calendario transcurridos desde el inicio de la cobertura del servicio de mantenimiento. El Plan de mantenimiento donde se detallarán las actividades a realizar con las fechas establecidas, deberá ser entregado al día siguiente de la suscripción del contrato.
A5.2	**SOPORTE TÉCNICO**
	Las actividades de soporte técnico deberán ser realizadas por el Contratista, por un plazo de 730 días calendario, el cual debe incluir: Se debe incluir soporte técnico (remoto o presencial), como primera instancia para la atención de requerimientos de los componentes que forman parte de la solución ofertada, las 24 horas del día, los 7 días de la semana y los 365 días del año. El tiempo de atención deberá ser como máximo (02) dos horas a partir de reportado el incidente. A fin de garantizar un óptimo nivel de servicio técnico, el proveedor debe contar con un sistema de mesa de ayuda propio, compuesto por: línea telefónica (fija y móvil) y correo electrónico corporativo. Bajo estas modalidades el Contratista debe garantizar el registro ante algún evento y/o incidente. El Contratista deberá garantizarlo para la suscripción del contrato, con una declaración jurada donde se indiquen los datos de contacto.
A5.3	**CAPACITACIÓN Y/O ENTRENAMIENTO**
	• Realizar una capacitación correspondiente a la solución ofertada de ANTIVIRUS y EDR y ANTISPAM (transferencia de conocimiento), para un mínimo de seis (06) personas Oficina de Informática del INEN, con una duración no menor de diez (10) horas. • El lugar de la capacitación será impartido en las oficinas del INEN, quien brindará el ambiente necesario y las facilidades para la capacitación presencial y/o virtual en cualquier plataforma de videoconferencia. • El dictado de la capacitación será previamente coordinado con el responsable designado por la Oficina de Informática del INEN. • La capacitación deberá ser dictada en el idioma español. • En un plazo no mayor a cinco (05) días de realizada la capacitación, se debe otorgar un certificado de participación a cada uno de los asistentes. • La capacitación estará a cargo del especialista considerado como personal clave (especialista en seguridad).
A6	**LUGAR Y PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN**
A6.1	**LUGAR**
	Oficina de Informática del INEN, sito en Av. Angamos Este N° 2520, Surquillo.
A6.2	**PLAZO**
	Plazo de la prestación principal, correspondiente a la entrega, instalación, configuración y puesta en funcionamiento de los componentes que forman parte de la solución ofertada: 15 días calendarios, contados a partir del día siguiente de la suscripción del contrato. **Plazo de vigencia de licencia:** 730 días calendarios, contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal. **Plazo de la prestación accesoria, correspondiente al mantenimiento preventivo:** 730 días calendarios, contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal. **Plazo de la prestación accesoria, correspondiente al soporte técnico:** 730 días calendarios, contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal. **Plazo de la prestación accesoria, correspondiente a la capacitación:** 10 calendarios, contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

A7	**REQUISITOS SEGÚN LEYES, REGLAMENTOS TÉCNICOS, NORMAS METROLÓGICAS Y/O SA-NITARIAS, REGLAMENTOS Y DEMÁS NORMAS**
	NORMAS SANITARIAS: Protocolos sanitarios y demás disposiciones que dicten los sectores y autoridades competentes, como parte de las medidas de prevención dictadas como consecuencia del Estado de Emergencia Nacional a consecuencia del brote del COVID-19. No se ha emitido, ninguna disposición u protocolo, al respecto, que regule la actividad destinada a proveer el objeto de contratación, como parte de las medidas de prevención dictadas como consecuencia del Estado de Emergencia Nacional a consecuencia del brote del COVID-19; sin embargo, de emitirse algún protocolo sanitario u otras disposiciones que dicten los sectores y autoridades competentes, el contratista deberá incluirlo como parte de su obligación en cumplimiento de este requerimiento; bajo su exclusiva responsabilidad. No obstante, el personal del contratista que ejecute las obligaciones señaladas en estas especificaciones técnicas, incluido el alcance de la garantía, deberá contar con equipos de protección personal (como guantes, mascarillas, lentes y/u otros que sean necesarios), para evitar el contagio de COVID-19); siendo responsabilidad exclusiva del contratista cumplir con esta disposición de protección ante la emergencia sanitaria declarada por el gobierno nacional.
B	**REQUISITOS Y RECURSOS DEL PROVEEDOR**
B1	**PERFIL DEL PERSONAL PROPUESTO**
	<u>Un (01) Jefe de Proyectos:</u> • Ingeniero titulado en la especialidad de Electricidad y/o Electrónica y/o Sistemas y/o Telemática y/o Informática y/o Computación. • Cuatro (04) años de experiencia en protección de virus informáticos, como Jefe de Proyectos realizando las siguientes actividades: administración y monitoreo de soluciones de seguridad. • Contar con una certificación oficial técnica en administración y monitoreo de antivirus, emitida por la marca de la funcionalidad antimalware ofertada. • Contar con una certificación oficial técnica, emitida por la marca de la funcionalidad antispam ofertada, siendo esto un requisito opcional. <u>Sus funciones serán las siguientes:</u> El jefe de proyectos será el responsable de dirigir el proyecto, para lo cual deberá encabezar el kick off donde presentará el plan de trabajo y los alcances de la solución ofertada. El Plan de trabajo y los alcances de la solución ofertada, deberá ser presentado al día siguiente de la suscripción del contrato. <u>Un (01) Coordinador en Seguridad:</u> • Ingeniero titulado en la especialidad de Electricidad y/o Electrónica y/o Sistemas y/o Telemática y/o Informática y/o Computación. • Cuatro (04) años de experiencia en protección de virus informáticos, como coordinador en seguridad realizando las siguientes actividades: administración, monitoreo y soporte de soluciones de seguridad. • Contar con una certificación oficial técnica en administración, monitoreo y soporte de antivirus, emitida por la marca de la funcionalidad antimalware ofertado. • Contar con una certificación oficial técnica, emitida por la marca de la funcionalidad antispam ofertada, siendo esto un requisito opcional. <u>Sus funciones serán las siguientes:</u> El coordinador en seguridad será el responsable de realizar las coordinaciones entre el personal del Contratista y el personal del INEN; además de supervisar cada etapa de instalación, configuración y puesta en funcionamiento de la solución ofertada. Los documentos que acrediten el perfil señalado para el Jefe de Proyectos y Coordinador en Seguridad se presentarán como parte de la documentación para la suscripción del contrato, y corresponderán a lo siguiente: copia simple del título profesional. Asimismo, la experiencia deberá ser acreditada 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, las cuales serán presentadas como parte de la documentación para la suscripción del contrato.

INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS
Av. Angamos Este 2520, Lima – 34 Telf.: 201-6500 Fax: 620-4991 Web: www.inen.sld.pe e-mail: postmaster@inen.sld.pe

	En cuanto, a las certificaciones, éstas deberán ser acreditadas con copia simple de constancia, certificados, u otros documentos según corresponda, las cuales serán presentadas como parte de la documentación para la suscripción del contrato. Un (01) Especialista en Seguridad: • Ingeniero o técnico en la especialidad electricidad y/o electrónica y/o sistemas y/o telemática y/o informatica y/o computación y/o ingeniería de software y/o redes y comunicaciones y/o redes y seguridad informática.[2] • Cuatro (04) años de experiencia en protección de virus informáticos, como especialista en seguridad realizando las siguientes actividades: instalación, configuración, administración, monitoreo y soporte de soluciones de seguridad. • Contar con una certificación oficial técnica en instalación, configuración, administración, monitoreo y soporte de antivirus, emitida por la marca de la funcionalidad antimalware ofertada. • Contar con una certificación oficial técnica, emitida por la marca de la funcionalidad antispam ofertada. El personal especialista en seguridad, se constituye como personal clave, y estará a cargo de la instalación, configuración y pue en funcionamiento de la solución ofertada. Deberá presentarse la copia simple de su título profesional o técnico, como parte de la documentación para la suscripción del contrato. Asimismo, las certificaciones deberán ser acreditadas con copia simple de constancia, certificados, u otros documentos según corresponda, las cuales serán presentadas como parte de la documentación para la suscripción del contrato. En cuanto a su experiencia, esta será acreditada como requisito de calificación.
B2	PERFIL DEL PROVEEDOR
	El proveedor debe estar certificado y/o acreditado por el fabricante de la marca de antivirus para comercializar los componentes que forman parte de la solución ofertada en el Perú; lo cual permite asegurar la procedencia legal acorde al cumplimiento de los procedimientos de garantía del fabricante en el Perú, y será acreditado con carta de la subsidiaria del fabricante en el Perú y/o carta del fabricante, la cual será presentada para la suscripción del contrato.[3]
C	OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN
C1	CONFIDENCIALIDAD
	El Contratista se compromete a guardar y reservar, respecto de los asuntos o información que resulte privilegiada o relevante, así como a no divulgar ni utilizar dicha información de manera indebida o en beneficio propio o de terceros, así como en perjuicio o desmedro del estado; hasta incluso después de finalizado la prestación, salvo que dicha información deje de ser sensible por haberse hecho de concomimiento público por el Instituto Nacional de Enfermedades Neoplásicas.
C2	CONFORMIDAD
	• La conformidad de la prestación principal será otorgada por la Oficina de Informática, previo informe de la Unidad Funcional de Servicios de Tecnología de Información y Comunicaciones, previa entrega, instalación y configuración de la solución oferta • La conformidad de la prestación por concepto al mantenimiento preventivo será otorgada por la Oficina de Informática, previo informe de la Unidad Funcional de Servicios de Tecnología de Información y Comunicaciones, luego de que el contratista haya realizado el mantenimiento preventivo, debiendo presentar para ello los reportes de informes de las incidencias solicitadas conteniendo los alcances señalados en el numeral A5.1 de las especificaciones técnicas. • La conformidad de la prestación por concepto al soporte técnico será otorgada por la Oficina de Informática, previo informe de la Unidad Funcional de Servicios de Tecnología de Información y Comunicaciones, luego de que el contratista haya realizado el soporte técnico, debiendo presentar para ello los reportes de informes de las incidencias solicitadas conteniendo los alcances señalados en el numeral A5.2 de las especificaciones técnicas. • La conformidad de la prestación por concepto a la capacitación será otorgada por la Oficina de Informática, previa presentación de los certificados de capacitación.
C3	FORMA DE PAGO
	Pago por la prestación principal: La Entidad realizará el pago de la contraprestación pactada a favor del contratista en PAGO ÚNICO, 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.

[2] Se modificó el literal B1 de acuerdo a la observación presentada por la empresa Micro Solutions TI S.A
[3] Se modificó el literal B2 de acuerdo a la consulta presentada por la empresa Micro Solutions TI S.A.

	Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación: • Recepción del Almacén General del INEN. • Informe del funcionario responsable de la Oficina de Informática, previo informe de la Unidad Funcional de Servicios de Tecnología de Información y Comunicaciones, emitiendo la conformidad de la prestación efectuada. • Comprobante de pago. **Pago por la prestación accesoria correspondiente al mantenimiento preventivo:** La Entidad realizará el pago del monto contratado por esta prestación en cuatro **PAGOS PARCIALES**, cada uno por igual monto; previa acta de conformidad. Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación: • Informe del funcionario responsable de la Oficina de Informática, previo informe de la Unidad Funcional de Servicios de Tecnología de Información y Comunicaciones, emitiendo la conformidad de la prestación efectuada • Comprobante de pago. **Pago por la prestación accesoria correspondiente al soporte técnico:** La Entidad realizará el pago del monto contratado por esta prestación en dos **PAGOS PARCIALES**, cada uno por igual monto; previa acta de conformidad, de acuerdo al siguiente detalle: Primer pago: Luego de haber transcurrido 365 días calendario de iniciado el servicio. Segundo pago: Luego de haber transcurrido 730 días calendario de iniciado el servicio. Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación: • Informe del funcionario responsable de la Oficina de Informática, previo informe de la Unidad Funcional de Servicios de Tecnología de Información y Comunicaciones, emitiendo la conformidad de la prestación efectuada. • Comprobante de pago. **Pago por la prestación accesoria correspondiente a Capacitación** La Entidad realizará el pago del monto contratado por esta prestación en **PAGO ÚNICO**, previa acta de conformidad. Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación: • Informe del funcionario responsable de la Oficina de Informática, emitiendo la conformidad de la prestación efectuada, por concepto de la capacitación. • Comprobante de pago.
C4	**RESPONSABILIDAD POR VICIOS OCULTOS**
	• La recepción conforme de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos de conformidad con el artículo 173° del Reglamento de la Ley de Contrataciones. • El plazo máximo de responsabilidad del contratista es de un (01) año contado a partir de cada conformidad otorgada por la ENTIDAD (artículo 40° de la Ley de Contrataciones del Estado). • El INEN se reserva el derecho de comprobar la veracidad, originalidad y cumplimiento de toda la información incluida en la propuesta del Postor a fin de aceptar o desestimar su propuesta.
C5	**OTRAS PENALIDADES APLICABLES**
	La entidad aplicará las siguientes penalidades:

PENALIDADES RESPECTO AL SERVICIO BRINDADO		
SOPORTE TÉCNICO	DEMORA EN EL TIEMPO DE ATENCIÓN MÁXIMA DE 2 HORAS	1% DE LA UIT POR CADA HORA O FRACCIÓN DE HORA, DE ATRASO INJUSTIFICADO
MANTENIMIENTOS PREVENTIVOS	NO EJECUCIÓN DEL PLAN DE MANTENIMIENTO PREVENTIVO PROPUESTO	2% DE LA UIT POR CADA DÍA DE ATRASO INJUSTIFICADO

Procedimiento de aplicación de penalidad: Para la aplicación de la penalidad, la Unidad Funcional de Tecnologías de la Información y Comunicaciones emitirá un informe comunicando las incidencias que ameritan la aplicación de penalidades, y de inmediato será derivado a la Oficina de Logística para el trámite correspondiente.

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	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/. 1´818,000.00 Un Millón Ochocientos Dieciocho Mil con 00/100 soles, por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se consideran bienes similares a los siguientes: Ventas de antivirus y/o venta de antispam. Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago[10], correspondientes a un máximo de veinte (20) contrataciones. 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 suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados. 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 compra o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de compra o de cancelación del comprobante de pago, según corresponda.

[10] 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".

	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** *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".*

C	**CAPACIDAD TÉCNICA Y PROFESIONAL**
C.1	**EXPERIENCIA DEL PERSONAL CLAVE**
	Requisitos: **Un (01) Especialista en Seguridad:** Cuatro (04) años de experiencia en protección de virus informáticos, como especialista en seguridad realizando las siguientes actividades: instalación, configuración, administración, monitoreo y soporte de soluciones de seguridad. Acreditación: La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

Importante

- *Si como resultado de una consulta u observación corresponde precisarse o ajustarse el requerimiento, se solicita la autorización del área usuaria y se pone de conocimiento de tal hecho a la dependencia que aprobó el expediente de contratación, de conformidad con el numeral 72.3 del artículo 72 del Reglamento.*

- *El cumplimiento de las Especificaciones Técnicas se realiza mediante la presentación de una declaración jurada. De ser el caso, adicionalmente la Entidad puede solicitar documentación que acredite el cumplimiento del algún componente de las características y/o requisitos funcionales. Para dicho efecto, consignará de manera detallada los documentos que deben presentar los postores en el literal e) del numeral 2.2.1.1 de esta sección de las bases.*

- *Los requisitos de calificación determinan si los postores cuentan con las capacidades necesarias para ejecutar el contrato, lo que debe ser acreditado documentalmente, y no mediante declaración jurada.*

CAPÍTULO IV
FACTORES DE EVALUACIÓN

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

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

FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A. PRECIO	
Evaluación: Se evaluará considerando el precio ofertado por el postor. Acreditación: Se acreditará mediante el documento que contiene el precio de la oferta **(Anexo N° 6).**	La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $Pi = \frac{Om \times PMP}{Oi}$ **i** = Oferta **Pi** = Puntaje de la oferta a evaluar **Oi** = Precio i **Om** = Precio de la oferta más baja **PMP** = Puntaje máximo del precio **100 puntos**
PUNTAJE TOTAL	**100 puntos**[11]

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 las Especificaciones Técnicas ni los requisitos de calificación.

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

CAPÍTULO V
PROFORMA DEL CONTRATO

Importante

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

Conste por el presente documento, la contratación de "ADQUISICIÓN DE SOLUCIÓN DE PROTECCIÓN DE VIRUS INFORMATICOS", que celebra de una parte INSTITUTO NACIONAL DE ENFERMEDADES NEOPLÁSICAS, en adelante LA ENTIDAD, con RUC Nº **20514964778**, con domicilio legal en AV. ANGAMOS ESTE N° 2520- SURQUILLO-LIMA, representada por [……], identificado con DNI Nº [……], y de otra parte [……], con RUC Nº [……], con domicilio legal en [……], inscrita en la Ficha N° [……] Asiento N° [……] del Registro de Personas Jurídicas de la ciudad de [……], debidamente representado por su Representante Legal, [……], con DNI N° [……], según poder inscrito en la Ficha N° [……], Asiento N° [……] del Registro de Personas Jurídicas de la ciudad de [……], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [……], el comité de selección adjudicó la buena pro de la **LICITACIÓN PÚBLICA N° 17-2022-INEN - PRIMERA CONVOCATORIA** para la contratación de "ADQUISICIÓN DE SOLUCIÓN DE PROTECCIÓN DE VIRUS INFORMATICOS", a [INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO], cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto "ADQUISICIÓN DE SOLUCIÓN DE PROTECCIÓN DE VIRUS INFORMATICOS".

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

CLÁUSULA CUARTA: DEL PAGO[12]

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en [INDICAR MONEDA], en SOLES, de acuerdo al siguiente detalle:

Pago por la prestación principal:

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en PAGOS UNICO, 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 efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Recepción del Almacén General del INEN.
- Informe del funcionario responsable de la Oficina de Informática, previo informe de la Unidad Funcional de Servicios de Tecnología de Información y Comunicaciones, emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.

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

Pago por la prestación accesoria correspondiente al mantenimiento preventivo:

La Entidad realizará el pago del monto contratado por esta prestación en cuatro PAGOS PARCIALES, cada uno por igual monto; previa acta de conformidad.

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

- Informe del funcionario responsable de la Oficina de Informática, previo informe de la Unidad Funcional de Servicios de Tecnología de Información y Comunicaciones, emitiendo la conformidad de la prestación efectuada
- Comprobante de pago.

Pago por la prestación accesoria correspondiente a Capacitación

La Entidad realizará el pago del monto contratado por esta prestación en PAGO ÚNICO, previa acta de conformidad.

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

- Informe del funcionario responsable de la Oficina de Informática, emitiendo la conformidad de la prestación efectuada, por concepto de la capacitación.
- Comprobante de pago.

Conforme con la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.

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

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

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

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

Los bienes materia de la presente convocatoria se entregarán de la siguiente manera:

- **Plazo de la prestación principal**, correspondiente a la entrega, instalación, configuración y puesta en funcionamiento de los componentes que forman parte de la solución ofertada: 15 días calendarios, contados a partir del día siguiente de la suscripción del contrato.

- **Plazo de vigencia de licencia**: 730 días calendarios, contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal.

- **Plazo de la prestación accesoria, correspondiente al mantenimiento preventivo**: 730 días calendarios, contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal.

- **Plazo de la prestación accesoria, correspondiente al soporte técnico**: 730 días calendarios, contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal.

- **Plazo de la prestación accesoria, correspondiente a la capacitación**: 10 calendarios,

contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal.

En concordancia con lo establecido en el expediente de contratación.

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

El presente contrato está conformado por las bases integradas, la oferta ganadora, así como los documentos derivados del procedimiento de selección que establezcan obligaciones para las partes.

CLÁUSULA SÉTIMA: GARANTÍAS

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

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

En el caso que corresponda, consignar lo siguiente:

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

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

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

CLÁUSULA NOVENA: RECEPCIÓN Y CONFORMIDAD DE LA PRESTACIÓN

La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La recepción será otorgada por el Almacén General del INEN (Para la Prestación Principal) y la conformidad será otorgada por:

- La conformidad de la prestación principal será otorgada por la Oficina de Informática, previo informe de la Unidad Funcional de Servicios de Tecnología de Información y Comunicaciones, previa entrega, instalación y configuración de la solución ofertada.

- La conformidad de la prestación por concepto al mantenimiento preventivo será otorgada por la Oficina de Informática, previo informe de la Unidad Funcional de Servicios de Tecnología de Información y Comunicaciones, luego de que el contratista haya realizado el mantenimiento preventivo, debiendo presentar para ello los reportes de informes de las incidencias solicitadas conteniendo los alcances señalados en el numeral A5.1 de las especificaciones técnicas.

- La conformidad de la prestación por concepto al soporte técnico será otorgada por la Oficina de Informática, previo informe de la Unidad Funcional de Servicios de Tecnología de Información y Comunicaciones, luego de que el contratista haya realizado el soporte técnico, debiendo presentar para ello los reportes de informes de las incidencias solicitadas conteniendo los alcances señalados en el numeral A5.2 de las especificaciones técnicas.

- La conformidad de la prestación por concepto a la capacitación será otorgada por la Oficina de Informática, previa presentación de los certificados de capacitación.

En el plazo máximo de [CONSIGNAR SIETE (7) DÍAS O MÁXIMO QUINCE (15) DÍAS, EN CASO SE REQUIERA EFECTUAR PRUEBAS QUE PERMITAN VERIFICAR EL CUMPLIMIENTO DE LA OBLIGACIÓN] días de producida la recepción.

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

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

CLÁUSULA UNDÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

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

CLÁUSULA DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

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

El plazo máximo de responsabilidad del contratista es de [CONSIGNAR TIEMPO EN AÑOS, NO MENOR DE UN (1) AÑO] año(s) contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA TERCERA: PENALIDADES

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

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

Donde:

F = 0.25 para plazos mayores a sesenta (60) días o;
F = 0.40 para plazos menores o iguales a sesenta (60) días.

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

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

Estas penalidades se deducen de los pagos a cuenta o del pago final, según corresponda; o si

fuera necesario, se cobra del monto resultante de la ejecución de la garantía de fiel cumplimiento.

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

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

CLÁUSULA DÉCIMA CUARTA: RESOLUCIÓN DEL CONTRATO

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

CLÁUSULA DÉCIMA QUINTA: RESPONSABILIDAD DE LAS PARTES

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

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

CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN

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

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

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

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

CLÁUSULA DÉCIMA SÉTIMA: MARCO LEGAL DEL CONTRATO

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

CLÁUSULA DÉCIMA OCTAVA: SOLUCIÓN DE CONTROVERSIAS

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

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

Facultativamente, cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 224 del Reglamento de la Ley de Contrataciones del Estado, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un

acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

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

CLÁUSULA DÉCIMA NOVENA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

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

CLÁUSULA VIGÉSIMA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

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

DOMICILIO DE LA ENTIDAD: [.....]

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

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

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

"LA ENTIDAD"

"EL CONTRATISTA"

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales[13].

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

ANEXOS

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 17-2022-INEN - PRIMERA CONVOCATORIA
Presente.-

El que se suscribe, [……..], postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], identificado con [CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD], con poder inscrito en la localidad de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] en la Ficha Nº [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA] Asiento Nº [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

Autorización de notificación por correo electrónico:

... [CONSIGNAR SÍ O NO] 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 subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.
4. Respuesta a la solicitud de acceso al expediente de contratación.
5. Notificación de la orden de compra[14]

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

[CONSIGNAR CIUDAD Y FECHA]

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

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

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

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
LICITACIÓN PÚBLICA N° 17-2022-INEN - PRIMERA CONVOCATORIA
Presente.-

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

Datos del consorciado 1			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
Correo electrónico :			

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

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

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

… [CONSIGNAR SÍ O NO] 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 subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.
4. Respuesta a la solicitud de acceso al expediente de contratación.
5. Notificación de la orden de compra[15]

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]

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

.....

Firma, Nombres y Apellidos del representante común del consorcio

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

ANEXO Nº 2

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

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 17-2022-INEN - PRIMERA CONVOCATORIA
Presente.-

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

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

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

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

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

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

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

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

ANEXO Nº 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 17-2022-INEN - PRIMERA CONVOCATORIA
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del procedimiento de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece la ADQUISICIÓN DE SOLUCIÓN DE PROTECCIÓN DE VIRUS INFORMATICOS, de conformidad con las Especificaciones Técnicas que se indican en el numeral 3.1 del Capítulo III de la sección específica de las bases y los documentos del procedimiento.

[CONSIGNAR CIUDAD Y FECHA]

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

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

ANEXO Nº 4

DECLARACIÓN JURADA DE PLAZO DE ENTREGA

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 17-2022-INEN - PRIMERA CONVOCATORIA
Presente.-

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de la referencia, me comprometo a entregar los bienes objeto del presente procedimiento de selección de acuerdo al siguiente detalle:

- **Plazo de la prestación principal**, correspondiente a la entrega, instalación, configuración y puesta en funcionamiento de los componentes que forman parte de la solución ofertada: 15 días calendarios, contados a partir del día siguiente de la suscripción del contrato.

- **Plazo de vigencia de licencia**: 730 días calendarios, contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal.

- **Plazo de la prestación accesoria**, **correspondiente al mantenimiento preventivo**: 730 días calendarios, contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal.

- **Plazo de la prestación accesoria**, **correspondiente al soporte técnico**: 730 días calendarios, contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal.

- **Plazo de la prestación accesoria, correspondiente a la capacitación**: 10 calendarios, contados a partir del día siguiente de haberse otorgado la conformidad por la prestación principal.

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO Nº 5

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

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 17-2022-INEN - PRIMERA CONVOCATORIA
Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta a la **LICITACIÓN PÚBLICA Nº 17-2022-INEN - PRIMERA CONVOCATORIA**.

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]	[%][16]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]	
2.	OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2]	[%][17]
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]	
	TOTAL OBLIGACIONES	100%[18]

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

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

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

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

ANEXO Nº 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 17-2022-INEN - PRIMERA CONVOCATORIA
Presente.-

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

CONCEPTO	CANTIDAD	PRECIO TOTAL
SOLUCIÓN DE PROTECCIÓN DE VIRUS INFORMATICOS.	1,800	
MANTENIMIENTO PREVENTIVO	4	
SOPORTE TECNICO	1	
CAPACITACIÓN Y/O ENTRENAMIENTO	1	
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 bien a contratar; excepto la de aquellos postores que gocen de alguna exoneración legal, no incluirán en el precio de su oferta los tributos respectivos.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

El postor que goce de alguna exoneración legal, debe indicar que su oferta no incluye el tributo materia de la exoneración, debiendo incluir el siguiente texto:

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

Importante para la Entidad

- *En caso de procedimientos según relación de ítems, consignar lo siguiente:*
  "El postor puede presentar el precio de su oferta en un solo documento o documentos independientes, en los ítems que se presente".

- *En caso de contrataciones que conllevan la ejecución de prestaciones accesorias, consignar lo siguiente:*
  "El postor debe detallar en el precio de su oferta, el monto correspondiente a la prestación principal y las prestaciones accesorias".

Incluir o eliminar, según corresponda

ANEXO Nº 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 17-2022-INEN - PRIMERA CONVOCATORIA
Presente.-

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

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [19]	FECHA DE LA CONFORMIDAD DE SER EL CASO[20]	EXPERIENCIA PROVENIENTE[21] DE:	MONEDA	IMPORTE[22]	TIPO DE CAMBIO VENTA[23]	MONTO FACTURADO ACUMULADO [24]
1										
2										
3										

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

[20] **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.

[21] 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"*.

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

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

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

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [19]	FECHA DE LA CONFORMIDAD DE SER EL CASO[20]	EXPERIENCIA PROVENIENTE[21] DE:	MONEDA	IMPORTE[22]	TIPO DE CAMBIO VENTA[23]	MONTO FACTURADO ACUMULADO [24]
4										
5										
6										
7										
8										
9										
10										
...										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO Nº 9

DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores
COMITÉ DE SELECCIÓN
LICITACIÓN PÚBLICA Nº 17-2022-INEN - PRIMERA CONVOCATORIA
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.*