

BASES ESTÁNDAR DE ADJUDICACIÓN SIMPLIFICADA PARA LA CONTRATACIÓN DE BIENES

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



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

SIMBOLOGÍA UTILIZADA:

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

CARACTERÍSTICAS DEL DOCUMENTO:

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

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

INSTRUCCIONES DE USO:

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

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

**BASES ESTÁNDAR DE ADJUDICACIÓN SIMPLIFICADA
PARA LA CONTRATACIÓN DE BIENES**

**ADJUDICACIÓN SIMPLIFICADA N°
014-2021-CENARES/MINSA**

PRIMERA CONVOCATORIA

**CONTRATACIÓN DE BIENES
ADQUISICION DE LICENCIAS DE SOFTWARE DE
ANTIVIRUS**

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.

B
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.

Al
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.

7
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)

[Handwritten marks: a stylized 'B' or 'P' at the top, followed by 'A' and 'D' below it.]

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, así como el literal a) del artículo 89 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 el numeral 72.4 del artículo 72 del Reglamento y el literal a) del artículo 89 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. FORMA DE PRESENTACIÓN DE OFERTAS

Las ofertas se presentan conforme lo establecido en el artículo 59 y en el artículo 90 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). 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.

1.7. 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 órgano encargado de las contrataciones o el comité de selección, según corresponda, 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, detallados en la sección específica de las bases. De no cumplir con lo requerido, la oferta se considera no admitida.

1.8. EVALUACIÓN DE LAS OFERTAS

La evaluación de las ofertas se realiza conforme a lo establecido en el numeral 74.1 y el literal a) del numeral 74.2 del artículo 74 del Reglamento.

En el supuesto de que dos (2) o más ofertas empaten, la determinación del orden de prelación de las ofertas empatadas se efectúa siguiendo estrictamente el orden establecido en el numeral 91.1 del artículo 91 del Reglamento.

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

1.9. 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.

1.10. 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.

1.11. RECHAZO DE LAS OFERTAS

Previo al otorgamiento de la buena pro, el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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 órgano encargado de las contrataciones o el comité de selección, según corresponda, revisa el cumplimiento de los requisitos de calificación de los postores que siguen en el orden de prelación, en caso las hubiere.

1.12. OTORGAMIENTO DE LA BUENA PRO

Definida la oferta ganadora, el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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.

1.13. CONSENTIMIENTO DE LA BUENA PRO

Cuando se hayan presentado dos (2) o más ofertas, el consentimiento de la buena pro se produce a los cinco (5) 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.

B

A

D

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 la Entidad convocante, y es conocido y resuelto por su Titular, cuando el valor estimado sea igual o menor a cincuenta (50) UIT. Cuando el valor estimado sea mayor a dicho monto, el recurso de apelación se presenta ante y es resuelto por el Tribunal de Contrataciones del Estado.

En los procedimientos de selección según relación de ítems, el valor estimado total del procedimiento determina ante quién se presenta el recurso de apelación.

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 órgano encargado de las contrataciones o el comité de selección, según corresponda, 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 órgano encargado de las contrataciones o el comité de selección, según corresponda.

- 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, o en la Unidad de Trámite Documentario de la Entidad, según corresponda.

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 cinco (5) 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 cinco (5) 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.

El contrato se perfecciona con la suscripción del documento que lo contiene, salvo en los contratos cuyo monto del valor estimado no supere los doscientos mil Soles (S/ 200,000.00), en los que se puede perfeccionar con la recepción de la orden de compra, conforme a lo previsto en la sección específica de las bases.

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 valor estimado del ítem corresponda al parámetro establecido en el párrafo anterior.

Importante

El órgano encargado de las contrataciones o el comité de selección, según corresponda, debe consignar en la sección específica de las bases la forma en que se perfeccionará el contrato, sea con la suscripción del contrato o la recepción de la orden de compra. En caso la Entidad perfeccione el contrato con la recepción de la orden de compra no debe incluir la proforma del contrato establecida en el Capítulo V de la sección específica de las bases.

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

Importante

En los contratos cuyos montos sean iguales o menores 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. Dicha excepción también aplica a 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 no superen el monto señalado anteriormente, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

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

Importante

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

Advertencia

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

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

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

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

Advertencia

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.

B

A

Y

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 : CENTRO NACIONAL DE ABASTECIMIENTO DE RECURSOS
ESTRATEGICOS EM SALUD
RUC N° : 20538298485
Domicilio legal : Jr. Nazca N° 548 – Jesus Maria
Teléfono: : 748-3030 – Anexo n° 6150
Correo electrónico: : rloayza@cenares.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación de la ADQUISICION DE LICENCIAS SOFTWARE DE ANTIVIRUS

N.º	DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA
01	Suscripción a licencia de Software Antivirus Corporativo para Estaciones	270	UNIDADES
02	Suscripción a la licencia de Software Antivirus Corporativo para Servidores	30	UNIDADES

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante MEMORANDO N° 1629-2021-DG-CENARES-MINSA el 28 de junio de 2021.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios

Importante

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

1.5. SISTEMA DE CONTRATACIÓN

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

1.6. MODALIDAD DE EJECUCIÓN

Llave en mano

1.7. DISTRIBUCIÓN DE LA BUENA PRO

No Aplica.

1.8. ALCANCES DEL REQUERIMIENTO

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

1.9. PLAZO DE ENTREGA

Los bienes materia de la presente convocatoria se entregarán en un plazo máximo de veinte (20) días calendarios, a partir de la suscripción del contrato para la implementación de las licencias de software y entrega del bien e instalación del servidor consola, el plazo será computado a partir del día siguiente de firmado el contrato y/o notificada la orden de compra, lo que ocurra primero, 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, este será entregado de forma gratuita. La entrega de las Bases podrá efectuarse de forma electrónica mediante el correo: rlaayza@cenare.gob.pe, o recabarlas en la Oficina de Adquisiciones del CENARES en Jr. Nazca 548 – Jesús María, en el horario de 08:30 a 16:30 horas

Importante

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

1.11. BASE LEGAL

- Decreto Supremo N° 162-2021-EF, modifican el Reglamento de la Ley de Contrataciones del Estado, aprobado mediante Decreto Supremo N° 344-2018-EF y dictan otras disposiciones
- Decreto Legislativo N°1440. Decreto Legislativo del Sistema Nacional de Presupuesto Público.
- Ley No 31084. Ley de Presupuesto del sector publico para el año fiscal 2021
- Ley No 31085. Ley de equilibrio financiero del presupuesto del sector publico para el año fiscal 2021
- Decreto Supremo N.º 082-2019-EF. TUO de la Ley N° 30225, Ley de Contrataciones del Estado, en adelante La Ley.
- Decreto Supremo N.º 344-2018-EF. Reglamento de la Ley de Contrataciones del Estado, en adelante el Reglamento.
- Decreto Supremo No 377-2019-EF. Que modifica el Reglamento de la Ley de Contrataciones del Estado, en adelante el Reglamento.
- Decreto Supremo N.º 004-2019-JUS. TUO de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- Directivas del OSCE.
- Texto Único Ordenado de la Ley No 27806, Ley de Transparencia y de Acceso a la Información
- Decreto Legislativo No 295. Código Civil.
- Resolución Directoral No 576-2021-CENARES/MINSA, que designa al Comité de Selección
- Demás normas complementarias y conexas con el objeto del presente procedimiento de selección.

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 documentos¹, 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 – PIDE² 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**)

¹ La omisión del índice no determina la no admisión de la oferta.

² 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 N° 4**)³
- f) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. (**Anexo N° 5**)
- g) El precio de la oferta en SOLES debe registrarse directamente en el formulario electrónico del SEACE.

Adicionalmente, se debe adjuntar el Anexo N° 6 en el caso de procedimientos convocados a precios unitarios.

En el caso de procedimientos convocados a suma alzada únicamente se debe adjuntar el Anexo N° 6, cuando corresponda indicar el monto de la oferta de la prestación accesoria o que el postor goza de alguna exoneración legal.

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

Importante

El órgano encargado de las contrataciones o el comité de selección según corresponda, 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) En el caso de microempresas y pequeñas empresas integradas por personas con discapacidad, o en el caso de consorcios conformados en su totalidad por estas empresas, deben presentar la constancia o certificado con el cual acredite su inscripción en el Registro de Empresas Promocionales para Personas con Discapacidad⁴.
- b) Solicitud de bonificación del cinco por ciento (5%) por tener la condición de micro y pequeña empresa (**Anexo N°9**).

Advertencia

El órgano encargado de las contrataciones o el comité de selección, según corresponda, 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”.

³ 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.

⁴ Dicho documento se tendrá en consideración en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

Importante para la Entidad

Esta disposición **solo** debe ser incluida en el caso de procedimientos de selección cuyo valor estimado sea igual o menor a cincuenta (50) UIT:

2.3. PRESENTACIÓN DEL RECURSO DE APELACIÓN


"El recurso de apelación se presenta ante la Unidad de Trámite Documentario de la Entidad.

En caso el participante o postor opte por presentar recurso de apelación y por otorgar la garantía mediante depósito en cuenta bancaria, se debe realizar el abono en:

N° de Cuenta : 00-068-309662
Banco : Banco de la Nación
N° CCI⁵ : 018-068-000-068-309662-72

2.4. 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)
 - b) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes, de ser el caso.
 - c) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y la entidad bancaria en el exterior.
 - d) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda. Emitido por SUNARP
 - e) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.
 - f) Domicilio para efectos de la notificación durante la ejecución del contrato, correo electrónico y número telefónico de contacto
 - g) Detalle de los precios unitarios del precio ofertado⁶.
 - h) Garantía comercial que el postor brinde entrara en vigencia a partir del inicio de la suscripción; y tendrá una duración de (24) meses

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE⁷ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).

⁵ En caso de transferencia interbancaria.




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

⁷ 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/>

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 cuyos montos sean iguales o menores 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. Dicha excepción también aplica a 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 no supere el monto señalado anteriormente, 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 Haya⁸.
 - La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.
- 
- 

2.5. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en Mesa de Partes del CENARES, sitio en Jr Nazca N° 548 – Jesus Maria, en el horario de lunes a viernes de 08:30 horas hasta las 16:30 horas.

⁸ Según lo previsto en la Opinión N° 009-2016/DTN.

2.6. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en único pago, el cual será realizado luego de haber sido emitida la conformidad por el Equipo de Informática del Centro de Gestión Administrativa del Centro Nacional de Abastecimiento en Recursos Estratégicos en Salud – CENARES..

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

- Factura (Remitente y Sunat) en original
- Copia Orden de Compra

Dicha documentación se debe presentar en mesa de partes del Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud, ubicado en Jr. Nazca 548 – Jesus Maria, en el horario de 08:30 a 16:30 horas.

B

A

M

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

Ministerio
de Salud

16
Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

ESPECIFICACIONES TÉCNICAS

SUSCRIPCIÓN A LICENCIA DE SOFTWARE ANTIVIRUS CORPORATIVO POR 24 MESES

1. AREA USUARIA

Centro de Gestión Administrativa – Equipo de Informática

2. DENOMINACIÓN DE LA CONTRATACIÓN

B
Suscripción a Licencia de software antivirus corporativo para la sede principal del Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud (CENARES).

3. OBJETO DE LA CONTRATACIÓN

F
Adquirir la suscripción a la licencia de Software Antivirus corporativo para reforzar la protección de los equipos de cómputo contra virus, troyanos, adware, spyware y otros programas maliciosos y poder instalarlos a todos los usuarios de CENARES.

4. FINALIDAD PÚBLICA

A
La finalidad del presente requerimiento es asegurar la disponibilidad y el correcto funcionamiento de los servicios, que garantice el cumplimiento de las metas y objetivos de nuestra Institución CENARES.

5. ASPECTOS GENERALES

M
Se requiere la adquisición, instalación, configuración e implementación de una solución antimalware y EDR.

6. OBJETIVOS DE LA CONTRATACIÓN

La presente contratación tiene como objetivo contar con un software antivirus que permitirá la seguridad y protección de los servicios y sistemas de usuario de la institución.



BICENTENARIO
PERÚ 2021



PERÚ Ministerio de Salud

Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud

7. DESCRIPCION BASICA DE LAS CARACTERISTICAS GENERALES

7.1. REQUERIMIENTO

N.º	DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA
01	Suscripción a licencia de Software Antivirus Corporativo para Estaciones	270	UNIDADES
02	Suscripción a la licencia de Software Antivirus Corporativo para Servidores	30	UNIDADES

7.2. CARACTERÍSTICAS ESTACIONES WINDOW

7.2.1. COMPATIBILIDAD

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 o superior
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Home / Pro / Educación / Enterprise

7.2.2. CARACTERÍSTICAS

7.2.2.1. Debe proporcionar las siguientes protecciones:

- Antimalware de archivos residente (antispysware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado.
- Antimalware de web (módulo para verificación de sitios y descargas contra virus).
- Antimalware de correo electrónico (módulo para verificación de correos recibidos y enviados, así como sus adjuntos).
- Firewall con IDS.



BICENTENARIO PERÚ 2021



PERÚ

Ministerio
de Salud

Centro Nacional de
Ajuste e Implementación de Recursos
Estratégicos en Salud

15

- Autoprotección (contra ataques a los servicios/procesos del antimalware).
- Control de dispositivos externos.
- Control de acceso a sitios por categoría.
- Control de ejecución de aplicativos.
- Control de vulnerabilidades de Windows y de los aplicativos instalados.

- 7.2.2.2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota.
- 7.2.2.3. Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo dos horas, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo).
- 7.2.2.4. Capacidad de automáticamente deshabilitar el Firewall de Windows (en caso de que exista) durante la instalación, para evitar incompatibilidad con el Firewall de la solución.
- 7.2.2.5. Capacidad de detección de presencia de antimalware de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación.
- 7.2.2.6. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antimalware. (ej.: "Win32.Trojan/banker") para que cualquier objeto detectado con el resultado elegido sea ignorado.
- 7.2.2.7. Capacidad de agregar aplicativos a una lista de "aplicativos confiables", donde las actividades de red, actividades de disco y acceso al registro de Windows no serán monitoreadas.
- 7.2.2.8. Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks).
- 7.2.2.9. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento.
- 7.2.2.10. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es posible de infección. El antimalware debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo.
- 7.2.2.11. Capacidad de verificar solamente archivos nuevos y modificados.
- 7.2.2.12. Capacidad de verificar objetos usando heurística.
- 7.2.2.13. Capacidad de agendar una pausa en la verificación.
- 7.2.2.14. Antes de cualquier intento de desinfección o exclusión permanente, el antimalware debe realizar un respaldo del objeto.
- 7.2.2.15. Capacidad de verificar correos electrónicos recibidos y enviados en



BICENTENARIO
PERÚ 2021



PERÚ

Ministerio
de Salud

Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

los protocolos POP3, IMAP, NNTP, SMTP y MAPL, así como conexiones cifradas (SSL) para POP3 y IMAP (SSL).

- 7.2.2.16. Capacidad de verificar enlaces introducidos en correos electrónicos contra pishings.
- 7.2.2.17. Capacidad de verificación del cuerpo del correo electrónico y adjuntos usando heurística.
- 7.2.2.18. En caso de que el correo electrónico contenga código que parece ser, pero no es definitivamente malicioso, este debe mantenerse en cuarentena.
- 7.2.2.19. Posibilidad de verificar solamente correos electrónicos recibidos, o recibidos y enviados.
- 7.2.2.20. Capacidad de filtrar adjuntos de correos electrónicos, borrándolos o renombrándolos de acuerdo con la configuración hecha por el administrador.
- 7.2.2.21. Capacidad de verificación de tráfico HTTP y cualquier script de Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas.
- 7.2.2.22. Capacidad de modificar las puertas monitoreadas por los módulos de web y correo electrónico.
- 7.2.2.23. En la verificación de tráfico web, en caso de que se encuentre código malicioso el programa debe:
- Preguntar qué hacer.
 - Bloquear el acceso al objeto y mostrar un mensaje sobre el bloqueo.
 - Permitir acceso al objeto.
- 7.2.2.24. El antimalware de web debe realizar la verificación de, como mínimo, dos maneras diferentes, a elección del administrador:
- Verificación *on-the-fly*, donde los datos se verifican mientras son recibidos en tiempo real.
 - Verificación de *buffer*, donde los datos se reciben y son almacenados para posterior verificación.
- 7.2.2.25. Posibilidad de agregar sitios de la web en una lista de exclusión, donde no serán verificados por el antimalware de web.
- 7.2.2.26. Debe tener módulo que analice las acciones de cada aplicación en ejecución en la computadora, grabando las acciones ejecutadas y comparándolas con secuencias características de actividades peligrosas. Tales registros de secuencias deben ser actualizados conjuntamente con las vacunas.





Centro Nacional de
Análisis de Riesgos
Estratégicos en Salud

14

- 7.2.2.27. Debe tener módulo que analice cada macro de VBA ejecutado, buscando señales de actividad maliciosa.
- 7.2.2.28. Debe contar con módulo que analice cualquier intento de edición, exclusión o grabación del registro, de forma que sea posible elegir claves específicas para ser monitoreadas y/o bloqueadas.
- 7.2.2.29. Debe tener módulo de bloqueo de Phishing, con actualizaciones incluidas en las vacunas, obtenidas por Anti-Phishing Working Group (<http://www.antiphishing.org/>).
- 7.2.2.30. Capacidad de distinguir diferentes subnets y brindar opción de activar o no el firewall para una subnet específica.
- 7.2.2.31. Debe tener módulo IDS (Intrusion Detection System) para protección contra port scans y exploración de vulnerabilidades de software. La base de datos de análisis debe actualizarse conjuntamente con las vacunas.
- 7.2.2.32. El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:
- Filtrado de paquetes: donde el administrador podrá elegir puertos, protocolos o direcciones de conexión que serán bloqueadas/permitidas.
 - Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados.
- 7.2.2.33. Debe tener módulo que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínimo:
- Discos de almacenamiento locales
 - Almacenamiento extraíble
 - Impresoras
 - CD/DVD
 - Drives de disquete
 - Modems
 - Dispositivos de cinta
 - Dispositivos multifuncionales
 - Lectores de smart card
 - Dispositivos de sincronización vía ActiveSync (Windows CE, Windows Mobile, etc.)
 - Wi-Fi
 - Adaptadores de red externos
 - Dispositivos MP3 o smartphones



BICENTENARIO
PERÚ 2021



PERÚ

Ministerio
de Salud

Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

- Dispositivos Bluetooth

- 7.2.2.34. Capacidad de liberar acceso a un dispositivo específico y usuarios específicos por un periodo de tiempo específico, sin la necesidad de deshabilitar la protección, sin deshabilitar el gerenciamiento central o de intervención local del administrador en la máquina del usuario.
- 7.2.2.35. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por usuario.
- 7.2.2.36. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por agendamiento.
- 7.2.2.37. Capacidad de configurar nuevos dispositivos por Class ID/Hardware ID.
- 7.2.2.38. Capacidad de limitar el acceso a sitios de internet por categoría, por contenido (video, audio, etc.), con posibilidad de configuración por usuario o grupos de usuarios y agendamiento.
- 7.2.2.39. Capacidad de limitar la ejecución de aplicativos por hash MD5, nombre del archivo, versión del archivo, nombre del aplicativo, versión del aplicativo, fabricante/desarrollador, categoría (ej.: navegadores, gestionado de descargas, juegos, aplicación de acceso remoto, etc.).
- 7.2.2.40. Capacidad de bloquear la ejecución de un aplicativo que esté en almacenamiento externo.
- 7.2.2.41. Capacidad de limitar el acceso de los aplicativos a recursos del sistema, como claves de registro y carpetas/archivos del sistema, por categoría, fabricante o nivel de confianza del aplicativo.
- 7.2.2.42. Capacidad de, en caso de epidemia, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.
- 7.2.2.43. Capacidad de, en caso de que la computadora cliente salga de la red corporativa, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.
- 7.2.2.44. La solución deberá tener la capacidad de realizar un borrado remoto de datos en dispositivos Windows.





PERÚ

Ministerio
de Salud

Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

13

7.3. CARACTERISTICAS ESTACIONES MAC OS X

7.3.1. COMPATILIDAD:

- macOS 10.13, 10.14, 10.15, o 11.0

7.3.2. CARACTERÍSTICAS:

- 7.3.2.1. Debe proporcionar protección residente para archivos (antispware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado.
- 7.3.2.2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota.
- 7.3.2.3. La instalación y primera ejecución del producto debe ser realizada sin necesidad de reiniciar la computadora, de modo que el producto funcione en toda su capacidad;
- 7.3.2.4. Debe contar con soportes a notificaciones utilizando Growl.
- 7.3.2.5. Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el periodo (alto, medio o bajo).
- 7.3.2.6. Capacidad de volver a la base de datos de la vacuna anterior.
- 7.3.2.7. Capacidad de barrer la cuarentena automáticamente después de cada actualización de vacunas.
- 7.3.2.8. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antimalware, (ej.: "Win32.Trojan/banker") para que cualquier objeto detectado con el resultado elegido sea ignorado;
- 7.3.2.9. Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks).
- 7.3.2.10. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es posible de infección. El antimalware debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo.
- 7.3.2.11. Capacidad de verificar solamente archivos nuevos y modificados.
- 7.3.2.12. Capacidad de verificar objetos usando heurística.
- 7.3.2.13. Capacidad de agendar una pausa en la verificación.
- 7.3.2.14. Antes de cualquier intento de desinfección o exclusión permanente, el





PERÚ
Ministerio
de Salud

Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

antimalware debe realizar un respaldo del objeto.

- 7.3.2.15. Capacidad de verificar archivos de formato de correo electrónico.
- 7.3.2.16. Posibilidad de trabajar con el producto por la línea de comando, con como mínimo opciones para actualizar las vacunas, iniciar un barrido, para el antimalware e iniciar el antimalware por la línea de comando.
- 7.3.2.17. Capacidad de ser instalado, removido y administrado por la misma consola central de gestión.

7.4. ESTACIONES DE TRABAJO LINUX

7.4.1. COMPATIBILIDAD

7.4.1.1. Sistemas de 64 bits:

- Ubuntu 16.04 LTS and later
- Red Hat Enterprise Linux 6.7 and later
- CentOS 6.7 and later
- Debian GNU / Linux 9.4 and later
- Debian GNU / Linux 10
- Linux Mint 18.2 and later
- Linux Mint 19 and later
- ALT 8 SP Workstation
- ALT 8 SP Server
- ALT Workstation 8
- ALT Workstation K 8
- ALT Server 8
- ALT Education 8
- ALT Server 9
- ALT Workstation 9
- ALT Education 9
- GosLinux 6.6
- Mageia 4

7.4.1.2. Sistemas de 32 bits:

- Ubuntu 16.04 LTS and later
- Ubuntu 18.04 LTS and later
- Red Hat Enterprise Linux 6.7 and later
- Red Hat Enterprise Linux 7.2 and later




BICENTENARIO
PERÚ 2021



PERÚ

Ministerio
de Salud

12
Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

- B
- Red Hat Enterprise Linux 8.0 and later
 - CentOS 6.7 and later
 - CentOS 7.2 and later
 - CentOS 8.0 and later
 - Debian GNU / Linux 9.4 and later
 - Debian GNU / Linux 10.1 and later
 - Oracle Linux 7.3 and later
 - Oracle Linux 8 and later
 - SUSE Linux Enterprise Server 12 SP3 and later
 - SUSE Linux Enterprise Server 15 and later
 - openSUSE Leap 15 and later
 - ALT 8 SP Workstation
 - ALT 8 SP Server
 - ALT Workstation 8
 - ALT Workstation K 8
 - ALT Server 8
 - ALT Education 8
 - ALT Workstation 9
 - ALT Server 9
 - ALT Education 9
 - Amazon Linux AMI
 - Linux Mint 18.2 and later
 - Linux Mint 19 and later
 - Astra Linux Special Edition, versión 1.5 (generic and PaX kernel)
 - Astra Linux Special Edition, versión 1.6 (generic and PaX kernel)
 - Astra Linux Common Edition, versión 2.12
 - OS ROSA Cobalt 7.3 for client systems
 - OS ROSA Cobalt 7.3 for server systems
 - GosLinux 6.6
 - GosLinux 7.2
 - AlterOS 7.5 and later
 - Pardus OS 19.1
 - RED OS 7.2
- B
- A
- M
- 



BICENTENARIO
PERÚ 2021



PERÚ

Ministerio
de Salud

Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

7.4.2. CARACTERÍSTICAS:

7.4.2.1. Debe proporcionar las siguientes protecciones:

- Antimalware de archivos residente (antispysware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado.
- Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.

7.4.2.2. Capacidad de configurar el permiso de acceso a las funciones del antimalware con, como mínimo, opciones para las siguientes funciones:

- Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);
- Gerenciamiento de respaldo: Creación de copias de los objetos infectados en un reservorio de respaldo antes del intento de desinfectar o eliminar tal objeto, siendo de esta manera posible la recuperación de objetos que contengan informaciones importantes;
- Gerenciamiento de cuarentena: Cuarentena de objetos sospechosos y corrompidos, guardando tales archivos en una carpeta de cuarentena;
- Verificación por agendamiento: búsqueda de archivos infectados y sospechosos (incluyendo archivos dentro de un rango especificado); análisis de archivos; desinfección o eliminación de objetos infectados.

7.4.2.3. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otro software.

7.4.2.4. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;

7.4.2.5. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es posible de infección. El antimalware debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;

7.4.2.6. Capacidad de verificar objetos usando heurística;

7.4.2.7. Control de dispositivos conectados con limitaciones de tiempo y de usuario a través de Samba Active Directory y Microsoft Active Directory en la tarea Control de dispositivos.

7.4.2.8. Administración del acceso de los usuarios a los dispositivos instalados o conectados por tipo de dispositivo y buses de conexión.

7.4.2.9. Escaneo del tráfico HTTP / HTTPS y FTP entrante del equipo del usuario



BICENTENARIO
PERÚ 2021



PERÚ

Ministerio
de Salud

Centro Nacional de
Atención en Infecciones de Transmisión Sexual
Estrategias en Salud

y la detección de direcciones web maliciosas y suplantación de identidad (phishing).

7.5. SERVIDORES WINDOWS

7.5.1. COMPATIBILIDAD

7.5.1.1. Sistemas de 32 bits

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 o superior.
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter SP2 o superior.
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 o superior.
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 o superior.

7.5.1.2. Sistemas de 64 bits

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 or later
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 or later
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 Standard / Premium SP1 or later
- Microsoft Small Business Server 2008 Standard / Premium
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 or later
- Windows Hyper-V Server 2008 R2 SP1 or later
- Microsoft Small Business Server 2011 Essentials / Standard
- Microsoft Windows MultiPoint Server 2011 Standard / Premium
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter
- Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter
- Microsoft Windows MultiPoint Server 2012 Standard / Premium
- Windows Storage Server 2012
- Windows Hyper-V Server 2012
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
- Windows Server 2012 R2 Core / Foundation / Essentials / Standard / Datacenter



BICENTENARIO
PERÚ 2021



PERÚ

Ministerio
de Salud

Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

- Windows Storage Server 2012 R2
- Windows Hyper-V Server 2012 R2
- Windows Server 2016 Essentials / Standard / Datacenter
- Windows Server 2016 MultiPoint
- Windows Server 2016 Core Standard / Datacenter
- Microsoft Windows MultiPoint Server 2016
- Windows Storage Server 2016
- Windows Hyper-V Server 2016
- Windows Server 2019 Essentials / Standard / Datacenter
- Windows Server 2019 Core
- Windows Storage Server 2019
- Windows Hyper-V Server 2019

7.5.2. CARACTERÍSTICAS

7.5.2.1. Debe proporcionar las siguientes protecciones:

- Antimalware de archivos residente (antispysware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
- Autoprotección contra ataques a los servicios/procesos del antimalware
- Firewall con IDS
- Control de vulnerabilidades de Windows y de los aplicativos instalados

7.5.2.2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota

7.5.2.3. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.

7.5.2.4. Capacidad de configurar el permiso de acceso a las funciones del antimalware con, como mínimo, opciones para las siguientes funciones:

- Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);
- Gerenciamiento de tarea (crear o excluir tareas de verificación)
- Lectura de configuraciones



BICENTENARIO
PERÚ 2021



PERÚ

Ministerio
de Salud



Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

10

- Modificación de configuraciones
- Gerenciamiento de respaldo y cuarentena
- Visualización de informes
- Gerenciamiento de informes
- Gerenciamiento de claves de licencia
- Gerenciamiento de permisos (agregar/excluir permisos superiores)

7.5.2.5. El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:

- Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas;
- Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados.

7.5.2.6. Capacidad de seleccionar por separado el número de procesos que ejecutarán funciones de barrido en tiempo real, el número de procesos que ejecutarán el barrido a demanda y el número máximo de procesos que pueden ser ejecutados en total.

7.5.2.7. Capacidad de reanudar automáticamente tareas de verificación que hayan sido interrumpidas por anomalías (corte de energía, errores, etc.)

7.5.2.8. Capacidad de automáticamente pausar y no iniciar tareas agendadas en caso de que el servidor esté funcionando con fuente ininterrumpida de energía (uninterruptible Power supply – UPS).

7.5.2.9. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otro software.

7.5.2.10. Capacidad de configurar niveles de verificación diferentes para cada carpeta, grupo de carpetas o archivos del servidor.



BICENTENARIO
PERÚ 2021



PERÚ

Ministerio
de Salud

Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

- 7.5.2.11. Capacidad de bloquear acceso al servidor de máquinas infectadas y cuando una máquina intenta grabar un archivo infectado en el servidor.
- 7.5.2.12. Capacidad de crear una lista de máquinas que nunca serán bloqueadas, aunque sean infectadas.
- 7.5.2.13. Capacidad de detección de presencia de antimalware de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación.
- 7.5.2.14. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antimalware, (ej.: "Win32.Trojan/banker") para que cualquier objeto detectado con el resultado elegido sea ignorado.
- 7.5.2.15. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;
- 7.5.2.16. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es posible de infección. El antimalware debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;
- 7.5.2.17. Capacidad de verificar solamente archivos nuevos y modificados;
- 7.5.2.18. Capacidad de elegir qué tipo de objeto compuesto será verificado (ej.: archivos comprimidos, archivos auto descompresores, .PST, archivos compactados por compactadores binarios, etc.).
- 7.5.2.19. Capacidad de verificar objetos usando heurística;
- 7.5.2.20. Capacidad de configurar diferentes acciones para diferentes tipos de





Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

amenazas.

- 7.5.2.21. Capacidad de agendar una pausa en la verificación;
- 7.5.2.22. Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo.
- 7.5.2.23. Antes de cualquier intento de desinfección o exclusión permanente, el antimalware debe realizar un respaldo del objeto.
- 7.5.2.24. Debe contar con módulo que analice cada script ejecutado, buscando señales de actividad maliciosa.
- 7.5.2.25. La solución deberá contar con protección Anti-Ransomware que actúe de forma proactiva ante un proceso de cifrado en las carpetas de red compartidas producido por un equipo remoto. Esta capacidad Anti-Ransomware debe permitir la definición granular de las carpetas a proteger.

7.6. CONSOLA DE GESTIÓN Y CARACTERÍSTICAS GENERALES

7.6.1. Compatibilidad para la consola On-Premise

- Microsoft Windows 10 20H2 32-bit/64-bit
- Microsoft Windows 10 20H1 32-bit/64-bit
- Microsoft Windows 10 Enterprise 2019 LTSC 32-bit/64-bit
- Microsoft Windows 10 Enterprise 2016 LTSC 32-bit/64-bit
- Microsoft Windows 10 Enterprise 2015 LTSC 32-bit/64-bit
- Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations RS5 (October 2018 Update, 1809) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-bit/64-bit
- Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-bit/64-bit
- Microsoft Windows 10 Pro 19H1 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations 19H1 32-bit/64-bit



BICENTENARIO
PERÚ 2021



PERÚ

Ministerio
de Salud



Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

- Microsoft Windows 10 Enterprise 19H1 32-bit/64-bit
- Microsoft Windows 10 Education 19H1 32-bit/64-bit
- Microsoft Windows 10 Pro 19H2 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations 19H2 32-bit/64-bit
- Microsoft Windows 10 Enterprise 19H2 32-bit/64-bit
- Microsoft Windows 10 Education 19H2 32-bit/64-bit
- Microsoft Windows 8.1 Pro 32-bit/64-bit
- Microsoft Windows 8.1 Enterprise 32-bit/64-bit
- Microsoft Windows 8 Pro 32-bit/64-bit
- Microsoft Windows 8 Enterprise 32-bit/64-bit
- Microsoft Windows 7 Professional with Service Pack 1 and higher 32-bit/64-bit
- Microsoft Windows 7 Enterprise/Ultimate with Service Pack 1 and higher 32-bit/64-bit
- Windows Server 2019 Standard 64-bit
- Windows Server 2019 Core 64-bit
- Windows Server 2019 Datacenter 64-bit
- Windows Server 2016 Server Standard RS3 (v1709) (LTSC/CBB) 64-bit
- Windows Server 2016 Server Datacenter RS3 (v1709) (LTSC/CBB) 64-bit
- Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSC/CBB) 64-bit
- Windows Server 2016 Standard (LTSC) 64-bit
- Windows Server 2016 Server Core (Installation Option) (LTSC) 64-bit
- Windows Server 2016 Datacenter (LTSC) 64-bit
- Windows Server 2012 R2 Standard 64-bit
- Windows Server 2012 R2 Server Core 64-bit
- Windows Server 2012 R2 Foundation 64-bit
- Windows Server 2012 R2 Essentials 64-bit
- Windows Server 2012 R2 Datacenter 64-bit
- Windows Server 2012 Standard 64-bit
- Windows Server 2012 Server Core 64-bit
- Windows Server 2012 Foundation 64-bit
- Windows Server 2012 Essentials 64-bit
- Windows Server 2012 Datacenter 64-bit
- Windows Storage Server 2016 64-bit
- Windows Storage Server 2012 R2 64-bit
- Windows Storage Server 2012 64-bit





Centro Nacional de
Asesoramiento de Recursos
Estratégicos en Salud

8

7.6.2. Características Generales

7.6.2.1. La solución debe disponer de una consola de gestión centralizada que

permita la instalación, configuración, actualización y administración de todas las soluciones ofertadas de manera integral, facilitando la gestión de la seguridad tanto en modalidad On-Premise como en la Nube.

7.6.2.2. Se debe acceder a la consola On-Premise vía WEB (HTTPS), MMC.

7.6.2.3. Compatibilidad con Windows Failover clustering u otra solución de alta disponibilidad en el caso de consola On-Premise.

7.6.2.4. Capacidad de eliminar remotamente cualquier solución de seguridad

(propia o de terceros) que esté presente en las estaciones y servidores, sin la necesidad de la contraseña de remoción de la actual solución de seguridad.

7.6.2.5. Capacidad de instalar remotamente la solución en las estaciones y

servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory;

7.6.2.6. Capacidad de instalar remotamente la solución de seguridad en

smartphones y tablets Android, utilizando estaciones como intermediadoras.

7.6.2.7. Capacidad de gestionar estaciones de trabajo y servidores de archivos

(tanto Windows como Linux y Mac) protegidos por la solución;

7.6.2.8. Capacidad de gestionar smartphones y tablets (tanto Android y iOS)

protegidos por la solución.

7.6.2.9. Capacidad de generar paquetes personalizados (autoejecutables)

conteniendo la licencia y configuraciones del producto.

7.6.2.10. Capacidad de actualizar los paquetes de instalación con las últimas





Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

vacunas, para que cuando el paquete sea utilizado en una instalación ya contenga las últimas vacunas lanzadas.

7.6.2.11. Capacidad de monitorear diferentes subnets de red con el objetivo de encontrar máquinas nuevas para que sean agregadas a la protección.

7.6.2.12. Capacidad de monitorear grupos de trabajos ya existentes y cualquier grupo de trabajo que sea creado en la red, a fin de encontrar máquinas nuevas para ser agregadas a la protección.

7.6.2.13. Capacidad de, al detectar equipos nuevos en el Active Directory,

subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antimalware instalado. En caso de no tenerlo, debe instalar el antimalware automáticamente.

7.6.2.14. Capacidad de agrupamiento de máquinas por características comunes

entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antimalware instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 2 días, etc.

7.6.2.15. Capacidad de definir políticas de configuraciones diferentes por grupos de estaciones, permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos.

7.6.2.16. Capacidad de importar la estructura de Active Directory para encontrar máquinas.

7.6.2.17. Debe proporcionar las siguientes informaciones de las computadoras:

- Si el antimalware está instalado.
- Si el antimalware ha iniciado.
- Si el antimalware está actualizado.
- Minutos/horas desde la última conexión de la máquina con el servidor administrativo.
- Minutos/horas desde la última actualización de vacunas.



BICENTENARIO
PERU 2021



PERÚ

Ministerio
de Salud

Centro Nacional de
Almacenamiento de Recursos
Estratégicos en Salud

- Fecha y horario de la última verificación ejecutada en la máquina.
 - Versión del antimalware instalado en la máquina.
 - Si es necesario reiniciar la computadora para aplicar cambios.
 - Fecha y horario de cuando la máquina fue encendida.
 - Cantidad de virus encontrados (contador) en la máquina.
 - Nombre de la computadora.
 - Dominio o grupo de trabajo de la computadora.
 - Fecha y horario de la última actualización de vacunas.
 - Sistema operativo con Service Pack.
 - Cantidad de procesadores.
 - Cantidad de memoria RAM.
 - Usuario(s) conectados en ese momento, con información de contacto (si están disponibles en el Active Directory).
 - Dirección IP.
 - Aplicativos instalados, inclusive aplicativos de terceros, con historial de instalación, conteniendo fecha y hora que el software fue instalado o removido.
 - Actualizaciones de Windows Updates instaladas.
 - Información completa de hardware conteniendo: procesadores, memoria, adaptadores de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD.
 - Vulnerabilidades de aplicativos instalados en la máquina.
- 7.6.2.18. Debe permitir bloquear que el usuario cambie las configuraciones de la solución instalada en las estaciones y servidores.
- 7.6.2.19. Capacidad de reconectar máquinas clientes al servidor administrativo más próximo, basado en reglas de conexión como:
- Cambio de gateway.
 - Cambio de subnet DNS.
 - Cambio de dominio.
 - Cambio de servidor DHCP.
 - Cambio de servidor DNS.
 - Cambio de servidor WINS.
 - Aparición de nueva subnet.
- 7.6.2.20. Capacidad de configurar políticas móviles para que cuando una computadora cliente esté fuera de la estructura de protección pueda actualizarse vía internet.
- 7.6.2.21. Capacidad de instalar otros servidores administrativos para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes.
- 7.6.2.22. Capacidad de interrelacionar servidores en estructura de jerarquía para obtener informes sobre toda la estructura de endpoints.



BICENTENARIO
PERÚ 2021



PERÚ Ministerio de Salud

Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

- 7.6.2.23. Capacidad de herencia de tareas y políticas en la estructura jerárquica de servidores administrativos.
- 7.6.2.24. Capacidad de elegir cualquier computadora cliente como repositorio de vacunas y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red.
- 7.6.2.25. Capacidad de hacer de este repositorio de vacunas un gateway para conexión con el servidor de administración, para que otras máquinas que no logran conectarse directamente al servidor puedan usar este gateway para recibir y enviar informaciones al servidor administrativo.
- 7.6.3. Capacidad de exportar informes para los siguientes tipos de archivos: PDF, HTML y XML.
- 7.6.4. Capacidad de generar traps SNMP para monitoreo de eventos;
- 7.6.5. Capacidad de enviar correos electrónicos para cuentas específicas en caso de algún evento.
- 7.6.6. Debe tener documentación de la estructura del banco de datos para generación de informes a partir de herramientas específicas de consulta (Crystal Reports, por ejemplo).
- 7.6.7. Capacidad de conectar máquinas vía Wake On Lan para realización de tareas (barrido, actualización, instalación, etc.), inclusive de máquinas que estén en subnets diferentes del servidor).
- 7.6.8. Capacidad de habilitar automáticamente una política en caso de que ocurra una infección masiva en la red (basado en cantidad de malware encontrados en determinado intervalo de tiempo).
- 7.6.9. Capacidad de realizar actualización incremental de vacunas en las computadoras clientes.
- 7.6.10. Capacidad de realizar inventario de hardware de todas las máquinas clientes.
- 7.6.11. Capacidad de realizar inventario de aplicativos de todas las máquinas clientes.
- 7.6.12. Capacidad de diferenciar máquinas virtuales de máquinas físicas.
- 7.6.13. La solución debe ser capaz de integrarse con soluciones SIEM.
- 7.6.14. La solución debe poder enviar notificaciones por correo electrónico.
- 7.6.15. La solución debe tener diferentes funciones de administrador que tengan una única interfaz / tablero durante el inicio de sesión y controladas por privilegios y derechos en función de sus roles (Administrador, Revisor, Investigador, etc.).





PERÚ
Ministerio
de Salud

Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

7.6.15.1. Capacidad de, en caso de epidemia, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.

7.7. EDR

- El fabricante debe de estar incluido dentro del framework MITRE ATT&CK EDR de elación de soluciones EDR.
- El fabricante debe tener experiencia probada en el descubrimiento de vulnerabilidades desconocidas, APTs, campañas de ciberespionaje y malware avanzado. Para ello debe haber publicado no menos de 100 documentos sobre campañas de APT y agentes de amenazas durante el último año.

7.7.1. COMPATIBILIDAD

- Windows 7 SP1 Home / Professional / Enterprise 32-bit / 64-bit
- Windows 8.1.1 Professional / Enterprise 32-bit / 64-bit
- Windows 10 RS3 (versión 1703) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS4 (versión 1803) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS5 (versión 1809) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS6 (versión 1903) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 19H2 (versión 1909) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 20H1 (versión 2004) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows Server 2008 R2 Foundation / Standard / Enterprise 64-bit
- Windows Server 2012 Foundation / Standard / Enterprise 64-bit
- Windows Server 2012 R2 Foundation / Standard / Enterprise 64-bit
- Windows Server 2016 Essentials / Standard / Datacenter 64-bit
- Windows Server 2019 Essentials / Standard / Datacenter 64-bit

7.7.2. CARACTERÍSTICAS

7.7.2.1. La solución debe admitir la detección automatizada de actividad maliciosa mediante soluciones Endpoint Protección.

7.7.2.2. La solución sugerida debe complementar la información del veredicto de



BICENTENARIO
PERU 2021



PERÚ

Ministerio
de Salud

Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

la solución Endpoint Protection con los artefactos del sistema sobre la detección.

7.7.2.3. La solución sugerida debe admitir la generación automática de indicadores de amenazas y/o compromiso (IoC) después de que se produzca la detección con la capacidad de aplicar una acción de respuesta.

7.7.2.4. La solución debe tener la capacidad de forzar la ejecución de un escaneo de IoC en todos los puntos finales con agentes EDR instalados.

7.7.2.5. La solución debe admitir la ejecución de análisis de IoC de acuerdo a una planificación indicada por el administrador o analista.

7.7.2.6. La solución debe admitir la importación de IoC de terceros en formato OpenIoC para su uso en el escaneo de los equipos.

7.7.2.7. La solución debe admitir el escaneo utilizando un conjunto de IoC generado automáticamente, cargado o externo (de terceros) para detectar amenazas no detectadas anteriormente.

7.7.2.8. La solución debe admitir la exportación de IoC generado por la solución a un archivo en formato OpenIoC.

7.7.2.9. La solución debe permitir la visibilidad detallada del incidente relacionada con la amenaza detectada en un endpoint.

7.7.2.10. La información detallada del incidente debe incluir al menos la siguiente información de la amenaza detectada:

- Gráfico de la cadena de desarrollo de amenazas (kill chain).
- Información sobre el dispositivo en el que se detecta la amenaza (nombre, dirección IP, dirección MAC, lista de usuarios, sistema operativo).
- Información general sobre la detección, incluido el modo de detección.
- Cambios de registro asociados a la detección.
- Historial de presencia de archivos en el dispositivo.
- Acciones de respuesta realizadas por la aplicación.

7.7.2.11. El gráfico de la cadena de desarrollo de amenazas (kill chain) debe proporcionar información visual sobre los objetos involucrados en el incidente, por ejemplo, sobre procesos clave en el dispositivo, conexiones de red, bibliotecas, registro, etc.

7.7.2.12. La información de un incidente debe presentar una vista detallada de los artefactos del sistema y los datos relacionados con el incidente para el análisis de la causa raíz:

- Proceso de spawning
- Conexiones de red
- Cambios en el registro
- Descarga de archivos



BICENTENARIO
PERÚ 2021

Documento Base para la Selección de Proponentes para Mujeres y Hombres
Anexo B.1. Documento Base, 2021 para la adjudicación

- Dropped de objetos

- 7.7.2.13. La solución debe admitir una comunicación segura entre la consola de administración y los puntos finales con el agente EDR.
- 7.7.2.14. La solución debe admitir la gestión del agente EDR a través de la interfaz de línea de comandos y por la consola.
- 7.7.2.15. La solución debe tener una función / módulo incorporado para recopilar los datos necesarios para la resolución de problemas, sin requerir un acceso físico al punto final.
- 7.7.2.16. El agente EDR debe tener un mecanismo de autodefensa para evitar que el agente modifique archivos relacionados con el agente / entradas de componentes del sistema, etc.

7.8. CIFRADO DE DATOS

7.8.1. COMPATIBILIDAD

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 or later.
- Windows 8 Professional / Enterprise.
- Windows 8.1 Professional / Enterprise.
- Windows 10 Home / Pro / Education / Enterprise.

7.8.2. CARACTERÍSTICAS

- 7.8.2.1. El acceso al recurso cifrado (archivo, carpeta o disco) debe ser garantizado aún en caso de que el usuario haya olvidado la contraseña, a través de procedimientos de recuperación.
- 7.8.2.2. Utilizar, como mínimo, un algoritmo AES con clave de 256 bits.
- 7.8.2.3. Capacidad de cifrar completamente el disco duro de la máquina, agregando un ambiente de preboot para autenticación del usuario.
- 7.8.2.4. Capacidad de utilizar Single Sign-On para la autenticación de preboot.
- 7.8.2.5. Permitir crear varios usuarios de autenticación preboot.
- 7.8.2.6. Capacidad de crear un usuario de autenticación preboot común con una contraseña igual para todas las máquinas a partir de la consola de manejo.
- 7.8.2.7. Capacidad de cifrar drives extraíbles de acuerdo con una regla creada por el administrador, con las opciones:
- Cifrar solamente los archivos nuevos que sean copiados para el disco extraíble, sin modificar los archivos ya existentes.
 - Cifrar todos los archivos individualmente.
 - Cifrar el dispositivo entero, de manera que no sea posible listar los archivos y carpetas almacenadas.

¹Decenio de la Igualdad de Oportunidades para Mujeres y Hombres
Año del Bicentenario del Perú: 200 años de independencia

- Cifrar el dispositivo en modo portátil, permitiendo acceder a los archivos en máquinas de terceros a través de una contraseña.
- 7.8.2.8. Capacidad de seleccionar carpetas y archivos (por tipo, o extensión) para ser cifradas automáticamente. En esta modalidad, los archivos deben estar accesibles para todas las máquinas gestionadas por la misma consola de manera transparente para los usuarios.
- 7.8.2.9. Capacidad de crear reglas de exclusiones para que ciertos archivos o carpetas nunca sean cifrados.
- 7.8.2.10. Capacidad de seleccionar aplicaciones que pueden o no tener acceso a los archivos cifrados.

7.9. GESTIÓN DE SISTEMAS

- 7.9.1. Gestión de Vulnerabilidades. Capacidad de detectar software de Microsoft y de terceros vulnerables, creando así un informe de software vulnerable.
- 7.9.2. Capacidad de corregir las vulnerabilidades de software de cualquier proveedor, haciendo la descarga centralizado o descentralizado de la corrección o actualización y aplicando esa corrección o actualización en las máquinas gestionadas de manera transparente para los usuarios.
- 7.9.3. Permite la planificación de fecha y hora para el despliegue de parches y actualizaciones, discriminando PCs y Servidores.
- 7.9.4. Sincronización con Microsoft Update, para el despliegue centralizado de Parches y actualizaciones Microsoft.
- 7.9.5. Capacidad de gestionar licencias de software de terceros.
- 7.9.6. Utilización de Puntos de distribución para el despliegue de parches y actualizaciones en entornos WAN para reducir la utilización de ancho de banda.
- 7.9.7. Capacidad de gestionar un inventario de hardware, con la posibilidad de registro de dispositivos (ej.: router, switch, proyector, accesorio, etc.), informando fecha de compra, lugar donde se encuentra, service tag, número de identificación y otros.
- 7.9.8. Capacidad de registro de información adicional en los activos de la empresa mediante campos personalizados.

8. PLAZO DE ENTREGA

El proveedor tendrá un plazo máximo de veinte (20) días calendario, a partir de la suscripción del contrato para la implementación de las licencias de software y entrega del bien e instalación del servidor consola, el

El presente documento es propiedad de CENARES, todos los derechos reservados. No se permite su reproducción sin el consentimiento escrito de CENARES.

plazo será computado a partir del día siguiente de firmado el contrato y/o notificada la orden de compra, lo que ocurra primero.

9. ENTREGABLES

Una vez culminada la instalación, configuración y pruebas se suscribirá un acta de implementación, para ello el proveedor deberá entregar la siguiente documentación técnica:

- Informe técnico de implementación.
- Procedimiento de solicitud de Soporte Técnico a nivel del Proveedor y del Fabricante.

10. GARANTÍA COMERCIAL

La garantía comercial que el postor brinde entrará en vigencia a partir del inicio de la suscripción; y tendrá una duración de (24) meses.

11. CAPACITACIÓN

- El instructor que impartirá la capacitación, deberá tener como mínimo grado profesional Técnico Titulado o Bachiller en las especialidades de: ingeniería de sistemas, informática, electrónica y/o ramas afines, acreditar documentariamente certificación del fabricante del producto de la solución ofertada, así como certificaciones y/o estudios en seguridad informática Ethical Hacking.
- Dicha capacitación se dictará en las instalaciones de la entidad y/o remoto según la coyuntura actual.
- Curso para 4 integrantes del Cenares en Alta Especialización en Gestión de TI (Itil 4 Fundam + Cobit 2019 Fund + CISSP) que consta de 101 horas lectivas e incluye Certificación.
- La capacitación podrá dictarse en un plazo posterior a la etapa de implementación y/o dentro del mismo periodo, pero será requisito para efectos de conformidad, contar con el registro del participante al curso.

12. FORMA DE PAGO

Único pago, el cual será realizado luego de haber sido emitida la conformidad por el Equipo de Informática del Centro de Gestión Administrativa del Centro Nacional de Abastecimiento en Recursos Estratégicos en Salud - CENARES.

Decenio de la Igualdad de Oportunidades para Mujeres y Hombres
Año del Bicentenario del Perú: 200 años de independencia

13. CONFORMIDAD

La conformidad será emitida por el Equipo de Informática del Centro de Gestión Administrativa del Centro Nacional de Abastecimiento en Recursos Estratégicos en Salud - CENARES previa presentación de los entregables y capacitación.

14. CONFIDENCIALIDAD

El contratista del servicio tiene y asume la obligación, tanto durante la vigencia del contrato, como después de su extinción, de guardar el secreto y la confidencialidad de cualquier información del Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud - CENARES a la que tenga acceso como consecuencia del desempeño de su servicio, quedando expresamente prohibido revelar dicha información.

Por lo expuesto en el párrafo precedente, el proveedor del servicio no podrá:

- Difundir, transmitir o revelar información a terceros.
- Usar la información recopilada para ofrecer, promocionar o brindar información sobre productos o servicios.
- Arrendar ni vender a terceros ningún dato de identificación personal que les haya sido proporcionado por el CENARES o como consecuencia del servicio brindado.
- Invitar al usuario a tomar parte en encuestas sobre productos, servicios, noticias o eventos.

15. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista será responsable por los vicios ocultos del bien ofertado, conforme a lo indicado en el Artículo 40° de la Ley de Contrataciones y 173° del Reglamento de la Ley de Contrataciones del Estado, por un plazo mínimo de dos (02) años, el cual será contabilizado a partir de la conformidad otorgada por el Equipo de Informática del CENARES.

16. PENALIDAD

El incumplimiento de la entrega de los equipos y prestación de los servicios, estará sujeto a la aplicación de penalidades, de conformidad con lo dispuesto en el artículo 162 de Reglamento.

3



Centro Nacional de
Atendimiento de Emergencias
Estratégicas en Salud

"La penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente fórmula:

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

Donde F tendrá los siguientes valores:

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

b) Para plazos mayores a sesenta (60) días:

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

b.2) Para obras: F = 0.15."

17. Otras consideraciones adicionales:

Durante el tiempo que dure el Estado de Emergencia declarado por el Gobierno a consecuencia del COVID-19, EL CONTRATISTA deberá cumplir con las siguientes condiciones del servicio:

- a. En la entrega de los bienes, así como los trabajos y/o visitas que se realicen en las instalaciones de la Entidad para la ejecución de la prestación, el personal del proveedor deberá cumplir con los protocolos sanitarios de operación ante el COVID-19 establecidos en el "Plan de vigilancia, prevención y control de COVID-19 en el trabajo" de la Entidad y lo dispuesto en la Resolución Ministerial N° 448-2020-MINSA.
- b. Deberá proporcionar permanentemente a su personal los equipos de protección personal e implementos de limpieza y desinfección, para la provisión del servicio; debiendo brindar (como mínimo) los siguientes:
 - Equipos de protección:
 - i. Mascarillas quirúrgicas
 - ii. Guantes de látex
 - iii. Lentes de seguridad





PERU

Ministerio
de Salud

Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

- Implementos de limpieza y desinfección: iv. Alcohol en gel o soluciones desinfectantes
- v. Jabón líquido y papel o toallas desechables, para el lavado de manos de su personal
- c. Control de temperatura corporal del personal.
- d. Guardar el distanciamiento social establecido en todo momento.
- e. Presentar el Plan de Vigilancia, Prevención y Control de COVID-19, al inicio de la entrega del bien (que cuente con la aprobación por parte del Comité de Seguridad y Salud en el Trabajo o el supervisor de Seguridad y Salud en el Trabajo de la empresa CONTRATISTA)
- f. Cumplir las instrucciones que se le den al ingresar y demás disposiciones que dicten los sectores y autoridades competentes al respecto.

18. REQUISITOS DE CALIFICACION

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/ 200,000.00 (Doscientos Mil con 00/100 soles), **por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.**

En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/ 21,000.00 (Veintiun mil con 00/100 soles), por la venta de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.





Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

2

Se consideran **servicios** similares a los siguientes: Servicio de venta y/o renovación de licencias antivirus, venta y/o renovación de licenciamientos de software de seguridad.

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 vócher 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 pago¹ 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.º 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

¹ 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".



BICENTENARIO
PERÚ 2021



PERÚ

Ministerio
de Salud

Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

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 una persona absorbida 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.

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

CAPACIDAD TECNICA Y PROFESIONAL

EXPERIENCIA DEL PERSONAL CLAVE

El postor deberá contar con el siguiente personal especialista encargado de la ejecución del proyecto, conforme a lo siguiente:

Requisito:



BICENTENARIO
PERÚ 2021



PERÚ

Ministerio
de Salud

Centro Nacional de
Abastecimiento de Recursos
Estratégicos en Salud

(01) Jefe de Proyecto:

Dos (02) años realizando actividades en: gestión de proyectos de tecnologías de la información y/o seguridad perimetral, y/o seguridad de información, y/o plan director 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.

(01) Especialista en Seguridad Endpoint.

Dos (02) años de experiencia prestando servicios de instalación y/o configuración y/o puesta en marcha y/o mantenimiento y/o soporte de la solución ofertada.

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.




ING. CAROLA RAMÍREZ DIOS DE CACHO
Responsable de Equipos de Informática
CENARES - MINSA



BICENTENARIO
PERÚ 2021

Importante

Para determinar que los postores cuentan con las capacidades necesarias para ejecutar el contrato, el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 200,000.00 (Doscientos mil con 00/100 soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/ 21,000.00 (Veintiun 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. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.</p> <p>Se consideran servicios similares a los siguientes: servicios de venta y/o renovación de licencias antivirus, venta y/o renovación de licenciamiento de software de seguridad</p> <p><u>Acreditación:</u></p> <p>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de 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 pago⁹ correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 7 referido a la Experiencia del Postor en la Especialidad.</p> <p>En el caso de suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.</p> <p>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las</p>

⁹ 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".

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° 8**.

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.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo N° 7** 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
	<p><u>Requisitos:</u></p> <p>(01) Jefe de Proyecto.</p> <p>Dos (02) años realizando actividades en: gestión de proyectos de tecnologías de la información y/o seguridad perimetral, y/o seguridad de información, y/o plan director de seguridad.</p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <p><u>Requisitos:</u></p> <p>(01) Especialista en Seguridad Endpoint.</p> <p>Dos (02) años de experiencia prestando servicios de instalación y/o configuración y/o puesta en marcha y/o mantenimiento y/o soporte de la solución ofertada</p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p>

Importante

- *El tiempo de experiencia mínimo debe ser razonable y congruente con el periodo en el cual el personal ejecutará las actividades para las que se le requiere, de forma tal que no constituya una restricción a la participación de postores.*
- *Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento y la fecha de emisión y nombres y apellidos de quien suscribe el documento.*
- *En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.*
- *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.*

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	
<p><u>Evaluación:</u> Se evaluará considerando el precio ofertado por el postor.</p> <p><u>Acreditación:</u> Se acreditará mediante registro en el SEACE o el documento que contiene el precio de la oferta (Anexo N°6), según corresponda.</p>	<p>La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula:</p> $P_i = \frac{O_m \times PMP}{O_i}$ <p>i = Oferta <i>P_i</i> = Puntaje de la oferta a evaluar <i>O_i</i> = Precio i <i>O_m</i> = Precio de la oferta más baja PMP = Puntaje máximo del precio</p> <p style="text-align: right;">100 puntos</p>

Importante

Los factores de evaluación elaborados por el órgano encargado de las contrataciones o el comité de selección, según corresponda, 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.

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 **ADQUISICION DE LICENCIAS DE SOFTWARE DE ANTIVIRUS**, que celebra de una parte el **CENTRO NACIONAL DE ABASTECIMIENTO DE RECURSOS ESTRATEGICOS EN SALUD - CENARES**, en adelante LA ENTIDAD, con RUC N° [...], con domicilio legal en [...], representada por [...], identificado con DNI N° [...], y de otra parte [...], con RUC N° [...], con domicilio legal en [...], inscrita en la Ficha N° [...], Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], debidamente representado por su Representante Legal, [...], con DNI N° [...], según poder inscrito en la Ficha N° [...], Asiento N° [...] del Registro de Personas Jurídicas de la ciudad de [...], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [...], el comité de selección, según corresponda, adjudicó la buena pro de la **ADJUDICACIÓN SIMPLIFICADA N° 014-2021-CENARES/MINSA** para la contratación de **ADQUISICION DE LICENCIAS DE SOFTWARE DE ANTIVIRUS**, 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 la **ADQUISICION DE LICENCIAS DE SOFTWARE DE ANTIVIRUS**.

N.º	DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA
01	Suscripción a licencia de Software Antivirus Corporativo para Estaciones	270	UNIDADES
02	Suscripción a la licencia de Software Antivirus Corporativo para Servidores	30	UNIDADES

7.2 CARACTERÍSTICAS ESTACIONES WINDOW (Como se indican en las especificaciones técnicas)

7.2.1. COMPATIBILIDAD

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 o superior
- Windows 8 Professional / Enterprise
- Windows 8.1 Professional / Enterprise
- Windows 10 Home / Pro / Educación / Enterprise

7.2.2. CARACTERÍSTICAS

7.2.2.1. Debe proporcionar las siguientes protecciones:

- Antimalware de archivos residente (antispymware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado.
- Antimalware de web (módulo para verificación de sitios y descargas contra virus).
- Antimalware de correo electrónico (módulo para verificación de correos recibidos y enviados, así como sus adjuntos).
- Firewall con IDS.
- Autoprotección (contra ataques a los servicios/procesos del antimalware).
- Control de dispositivos externos.
- Control de acceso a sitios por categoría.
- Control de ejecución de aplicativos.
- Control de vulnerabilidades de Windows y de los aplicativos instalados.

7.2.2.2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota.

7.2.2.3. Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo dos horas, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo).

7.2.2.4. Capacidad de automáticamente deshabilitar el Firewall de Windows (en caso de que exista) durante la instalación, para evitar incompatibilidad con el Firewall de la solución.

7.2.2.5. Capacidad de detección de presencia de antimalware de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación.

7.2.2.6. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antimalware, (ej.: "Win32.Trojan/banker") para que cualquier objeto detectado con el resultado elegido sea ignorado.

7.2.2.7. Capacidad de agregar aplicativos a una lista de "aplicativos confiables", donde las actividades de red, actividades de disco y acceso al registro de Windows no serán monitoreadas.

7.2.2.8. Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks).

7.2.2.9. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento.

7.2.2.10. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es posible de infección. El antimalware debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo.

7.2.2.11. Capacidad de verificar solamente archivos nuevos y modificados.

7.2.2.12. Capacidad de verificar objetos usando heurística.

7.2.2.13. Capacidad de agendar una pausa en la verificación.

7.2.2.14. Antes de cualquier intento de desinfección o exclusión permanente, el antimalware debe realizar un respaldo del objeto.

7.2.2.15. Capacidad de verificar correos electrónicos recibidos y enviados en los protocolos POP3, IMAP, NNTP, SMTP y MAPI, así como conexiones cifradas (SSL) para POP3 y IMAP (SSL).

7.2.2.16. Capacidad de verificar enlaces introducidos en correos electrónicos contra pishings.

7.2.2.17. Capacidad de verificación del cuerpo del correo electrónico y adjuntos usando heurística.

7.2.2.18. En caso de que el correo electrónico contenga código que parece ser, pero no es definitivamente malicioso, este debe mantenerse en cuarentena.

- 7.2.2.19. Posibilidad de verificar solamente correos electrónicos recibidos, o recibidos y enviados.
- 7.2.2.20. Capacidad de filtrar adjuntos de correos electrónicos, borrándolos o renombrándolos de acuerdo con la configuración hecha por el administrador.
- 7.2.2.21. Capacidad de verificación de tráfico HTTP y cualquier script de Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas.
- 7.2.2.22. Capacidad de modificar las puertas monitoreadas por los módulos de web y correo electrónico.
- 7.2.2.23. En la verificación de tráfico web, en caso de que se encuentre código malicioso el programa debe:
- Preguntar qué hacer.
 - Bloquear el acceso al objeto y mostrar un mensaje sobre el bloqueo.
 - Permitir acceso al objeto.
- 7.2.2.24. El antimalware de web debe realizar la verificación de, como mínimo, dos maneras diferentes, a elección del administrador:
- Verificación *on-the-fly*, donde los datos se verifican mientras son recibidos en tiempo real.
 - Verificación de *buffer*, donde los datos se reciben y son almacenados para posterior verificación.
- 7.2.2.25. Posibilidad de agregar sitios de la web en una lista de exclusión, donde no serán verificados por el antimalware de web.
- 7.2.2.26. Debe tener módulo que analice las acciones de cada aplicación en ejecución en la computadora, grabando las acciones ejecutadas y comparándolas con secuencias características de actividades peligrosas. Tales registros de secuencias deben ser actualizados conjuntamente con las vacunas.
- 7.2.2.27. Debe tener módulo que analice cada macro de VBA ejecutado, buscando señales de actividad maliciosa.
- 7.2.2.28. Debe contar con módulo que analice cualquier intento de edición, exclusión o grabación del registro, de forma que sea posible elegir claves específicas para ser monitoreadas y/o bloqueadas.
- 7.2.2.29. Debe tener módulo de bloqueo de Phishing, con actualizaciones incluidas en las vacunas, obtenidas por Anti-Phishing Working Group (<http://www.antiphishing.org/>).
- 7.2.2.30. Capacidad de distinguir diferentes subnets y brindar opción de activar o no el firewall para una subnet específica.
- 7.2.2.31. Debe tener módulo IDS (Intrusion Detection System) para protección contra port scans y exploración de vulnerabilidades de software. La base de datos de análisis debe actualizarse conjuntamente con las vacunas.
- 7.2.2.32. El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:
- Filtrado de paquetes: donde el administrador podrá elegir puertos, protocolos o direcciones de conexión que serán bloqueadas/permitidas.
 - Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados.
- 7.2.2.33. Debe tener módulo que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínimo:
- Discos de almacenamiento locales

- Almacenamiento extraíble
- Impresoras
- CD/DVD
- Drives de disquete
- Modems
- Dispositivos de cinta
- Dispositivos multifuncionales
- Lectores de smart card
- Dispositivos de sincronización vía ActiveSync (Windows CE, Windows Mobile, etc.)
- Wi-Fi
- Adaptadores de red externos
- Dispositivos MP3 o smartphones
- Dispositivos Bluetooth

- 7.2.2.34. Capacidad de liberar acceso a un dispositivo específico y usuarios específicos por un período de tiempo específico, sin la necesidad de deshabilitar la protección, sin deshabilitar el gerenciamiento central o de intervención local del administrador en la máquina del usuario.
- 7.2.2.35. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por usuario.
- 7.2.2.36. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por agendamiento.
- 7.2.2.37. Capacidad de configurar nuevos dispositivos por Class ID/Hardware ID.
- 7.2.2.38. Capacidad de limitar el acceso a sitios de internet por categoría, por contenido (video, audio, etc.), con posibilidad de configuración por usuario o grupos de usuarios y agendamiento.
- 7.2.2.39. Capacidad de limitar la ejecución de aplicativos por hash MD5, nombre del archivo, versión del archivo, nombre del aplicativo, versión del aplicativo, fabricante/desarrollador, categoría (ej.: navegadores, gestionado de descargas, juegos, aplicación de acceso remoto, etc.).
- 7.2.2.40. Capacidad de bloquear la ejecución de un aplicativo que esté en almacenamiento externo.
- 7.2.2.41. Capacidad de limitar el acceso de los aplicativos a recursos del sistema, como claves de registro y carpetas/archivos del sistema, por categoría, fabricante o nivel de confianza del aplicativo.
- 7.2.2.42. Capacidad de, en caso de epidemia, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.
- 7.2.2.43. Capacidad de, en caso de que la computadora cliente salga de la red corporativa, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.
- 7.2.2.44. La solución deberá tener la capacidad de realizar un borrado remoto de datos en dispositivos Windows.

7.3. CARACTERISTICAS ESTACIONES MAC OS X

7.3.1. COMPATILIDAD:

- macOS 10.13, 10.14, 10.15, o 11.0

7.3.2. CARACTERÍSTICAS:

- 7.3.2.1. Debe proporcionar protección residente para archivos (antispymware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado.
- 7.3.2.2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota.
- 7.3.2.3. La instalación y primera ejecución del producto debe ser realizada sin necesidad de reiniciar la computadora, de modo que el producto funcione en toda su capacidad;
- 7.3.2.4. Debe contar con soportes a notificaciones utilizando Growl.
- 7.3.2.5. Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo).
- 7.3.2.6. Capacidad de volver a la base de datos de la vacuna anterior.
- 7.3.2.7. Capacidad de barrer la cuarentena automáticamente después de cada actualización de vacunas.
- 7.3.2.8. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antimalware, (ej.: "Win32.Trojan/banker") para que cualquier objeto detectado con el resultado elegido sea ignorado;
- 7.3.2.9. Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks).
- 7.3.2.10. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es posible de infección. El antimalware debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo.
- 7.3.2.11. Capacidad de verificar solamente archivos nuevos y modificados.
- 7.3.2.12. Capacidad de verificar objetos usando heurística.
- 7.3.2.13. Capacidad de agendar una pausa en la verificación.
- 7.3.2.14. Antes de cualquier intento de desinfección o exclusión permanente, el antimalware debe realizar un respaldo del objeto.
- 7.3.2.15. Capacidad de verificar archivos de formato de correo electrónico.
- 7.3.2.16. Posibilidad de trabajar con el producto por la línea de comando, con como mínimo opciones para actualizar las vacunas, iniciar un barrido, para el antimalware e iniciar el antimalware por la línea de comando.
- 7.3.2.17. Capacidad de ser instalado, removido y administrado por la misma consola central de gestión.

7.4. ESTACIONES DE TRABAJO LINUX




7.4.1. COMPATIBILIDAD

7.4.1.1. Sistemas de 64 bits:

- Ubuntu 16.04 LTS and later
- Red Hat Enterprise Linux 6.7 and later
- CentOS 6.7 and later
- Debian GNU / Linux 9.4 and later
- Debian GNU / Linux 10
- Linux Mint 18.2 and later
- Linux Mint 19 and later
- ALT 8 SP Workstation

- ALT 8 SP Server
- ALT Workstation 8
- ALT Workstation K 8
- ALT Server 8
- ALT Education 8
- ALT Server 9
- ALT Workstation 9
- ALT Education 9
- GosLinux 6.6
- Mageia 4

7.4.1.2. Sistemas de 32 bits:

- 
- 
- 
- Ubuntu 16.04 LTS and later
 - Ubuntu 18.04 LTS and later
 - Red Hat Enterprise Linux 6.7 and later
 - Red Hat Enterprise Linux 7.2 and later
 - Red Hat Enterprise Linux 8.0 and later
 - CentOS 6.7 and later
 - CentOS 7.2 and later
 - CentOS 8.0 and later
 - Debian GNU / Linux 9.4 and later
 - Debian GNU / Linux 10.1 and later
 - Oracle Linux 7.3 and later
 - Oracle Linux 8 and later
 - SUSE Linux Enterprise Server 12 SP3 and later
 - SUSE Linux Enterprise Server 15 and later
 - openSUSE Leap 15 and later
 - ALT 8 SP Workstation
 - ALT 8 SP Server
 - ALT Workstation 8
 - ALT Workstation K 8
 - ALT Server 8
 - ALT Education 8
 - ALT Workstation 9
 - ALT Server 9
 - ALT Education 9
 - Amazon Linux AMI
 - Linux Mint 18.2 and later
 - Linux Mint 19 and later
 - Astra Linux Special Edition, versión 1.5 (generic and PaX kernel)
 - Astra Linux Special Edition, versión 1.6 (generic and PaX kernel)
 - Astra Linux Common Edition, versión 2.12
 - OS ROSA Cobalt 7.3 for client systems
 - OS ROSA Cobalt 7.3 for server systems
 - GosLinux 6.6
 - GosLinux 7.2
 - AlterOS 7.5 and later
 - Pardus OS 19.1
 - RED OS 7.2

7.4.2. CARACTERÍSTICAS:

7.4.2.1. Debe proporcionar las siguientes protecciones:

- Antimalware de archivos residente (antispymware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado.
- Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.

7.4.2.2. Capacidad de configurar el permiso de acceso a las funciones del antimalware con, como mínimo, opciones para las siguientes funciones:

- Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);
- Gerenciamiento de respaldo: Creación de copias de los objetos infectados en un reservorio de respaldo antes del intento de desinfectar o eliminar tal objeto, siendo de esta manera posible la recuperación de objetos que contengan informaciones importantes;
- Gerenciamiento de cuarentena: Cuarentena de objetos sospechosos y corrompidos, guardando tales archivos en una carpeta de cuarentena;
- Verificación por agendamiento: búsqueda de archivos infectados y sospechosos (incluyendo archivos dentro de un rango especificado); análisis de archivos; desinfección o eliminación de objetos infectados.

7.4.2.3. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otro software.

7.4.2.4. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;

7.4.2.5. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es posible de infección. El antimalware debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;

7.4.2.6. Capacidad de verificar objetos usando heurística;

7.4.2.7. Control de dispositivos conectados con limitaciones de tiempo y de usuario a través de Samba Active Directory y Microsoft Active Directory en la tarea Control de dispositivos.

7.4.2.8. Administración del acceso de los usuarios a los dispositivos instalados o conectados por tipo de dispositivo y buses de conexión.

7.4.2.9. Escaneo del tráfico HTTP / HTTPS y FTP entrante del equipo del usuario y la detección de direcciones web maliciosas y suplantación de identidad (phishing).

7.5. SERVIDORES WINDOWS

7.5.1. COMPATIBILIDAD

7.5.1.1. Sistemas de 32 bits

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 o superior.
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter SP2 o superior.
- Windows Server 2008 Standard / Enterprise / Datacenter SP1 o superior.
- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 o superior.

7.5.1.2. Sistemas de 64 bits

- Windows Server 2003 Standard / Enterprise / Datacenter SP2 or later
- Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 or later

- Windows Server 2008 Core Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 Standard / Premium SP1 or later
- Microsoft Small Business Server 2008 Standard / Premium
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter SP1 or later
- Windows Server 2008 R2 Core Standard / Enterprise / Datacenter SP1 or later
- Windows Hyper-V Server 2008 R2 SP1 or later
- Microsoft Small Business Server 2011 Essentials / Standard
- Microsoft Windows MultiPoint Server 2011 Standard / Premium
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter
- Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter
- Microsoft Windows MultiPoint Server 2012 Standard / Premium
- Windows Storage Server 2012
- Windows Hyper-V Server 2012
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter
- Windows Server 2012 R2 Core / Foundation / Essentials / Standard / Datacenter
- Windows Storage Server 2012 R2
- Windows Hyper-V Server 2012 R2
- Windows Server 2016 Essentials / Standard / Datacenter
- Windows Server 2016 MultiPoint
- Windows Server 2016 Core Standard / Datacenter
- Microsoft Windows MultiPoint Server 2016
- Windows Storage Server 2016
- Windows Hyper-V Server 2016
- Windows Server 2019 Essentials / Standard / Datacenter
- Windows Server 2019 Core
- Windows Storage Server 2019
- Windows Hyper-V Server 2019

7.5.2. CARACTERÍSTICAS

7.5.2.1. Debe proporcionar las siguientes protecciones:

- Antimalware de archivos residente (antispymware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
- Autoprotección contra ataques a los servicios/procesos del antimalware
- Firewall con IDS
- Control de vulnerabilidades de Windows y de los aplicativos instalados

7.5.2.2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación

local como en la instalación remota

7.5.2.3. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada

hora.

7.5.2.4. Capacidad de configurar el permiso de acceso a las funciones del

antimalware con, como mínimo, opciones para las siguientes funciones:

- Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);
- Gerenciamiento de tarea (crear o excluir tareas de verificación)
- Lectura de configuraciones
- Modificación de configuraciones

- Gerenciamiento de respaldo y cuarentena
- Visualización de informes
- Gerenciamiento de informes
- Gerenciamiento de claves de licencia
- Gerenciamiento de permisos (agregar/excluir permisos superiores)

7.5.2.5. El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:

- Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas;
- Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados.

7.5.2.6. Capacidad de seleccionar por separado el número de procesos que ejecutarán funciones de barrido en tiempo real, el número de procesos que ejecutarán el barrido a demanda y el número máximo de procesos que pueden ser ejecutados en total.

7.5.2.7. Capacidad de reanudar automáticamente tareas de verificación que hayan sido interrumpidas por anomalías (corte de energía, errores, etc.)

7.5.2.8. Capacidad de automáticamente pausar y no iniciar tareas agendadas en caso de que el servidor esté funcionando con fuente ininterrumpida de energía (uninterruptible Power supply – UPS).

7.5.2.9. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otro software.

7.5.2.10. Capacidad de configurar niveles de verificación diferentes para cada carpeta, grupo de carpetas o archivos del servidor.

7.5.2.11. Capacidad de bloquear acceso al servidor de máquinas infectadas y cuando una máquina intenta grabar un archivo infectado en el servidor.

7.5.2.12. Capacidad de crear una lista de máquinas que nunca serán bloqueadas, aunque sean infectadas.

7.5.2.13. Capacidad de detección de presencia de antimalware de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación.

7.5.2.14. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar

objetos a la lista de exclusión de acuerdo con el resultado del antimalware, (ej.: "Win32.Trojan/banker") para que cualquier objeto detectado con el resultado elegido sea ignorado.

7.5.2.15. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;

7.5.2.16. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es posible de infección. El antimalware debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;

7.5.2.17. Capacidad de verificar solamente archivos nuevos y modificados;

7.5.2.18. Capacidad de elegir qué tipo de objeto compuesto será verificado (ej.: archivos comprimidos, archivos auto descompresores, .PST, archivos compactados por compactadores binarios, etc.).

7.5.2.19. Capacidad de verificar objetos usando heurística;

7.5.2.20. Capacidad de configurar diferentes acciones para diferentes tipos de amenazas.

7.5.2.21. Capacidad de agendar una pausa en la verificación;

7.5.2.22. Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo.

7.5.2.23. Antes de cualquier intento de desinfección o exclusión permanente, el antimalware debe realizar un respaldo del objeto.

7.5.2.24. Debe contar con módulo que analice cada script ejecutado, buscando señales de actividad maliciosa.

7.5.2.25. La solución deberá contar con protección Anti-Ransomware que actúe de forma proactiva ante un proceso de cifrado en las carpetas de red compartidas producido por un equipo remoto. Esta capacidad Anti-Ransomware debe permitir la definición granular de las carpetas a proteger.

7.6. CONSOLA DE GESTIÓN Y CARACTERÍSTICAS GENERALES

7.6.1. **Compatibilidad para la consola On-Premise**

- Microsoft Windows 10 20H2 32-bit/64-bit

- Microsoft Windows 10 20H1 32-bit/64-bit
- Microsoft Windows 10 Enterprise 2019 LTSC 32-bit/64-bit
- Microsoft Windows 10 Enterprise 2016 LTSC 32-bit/64-bit
- Microsoft Windows 10 Enterprise 2015 LTSC 32-bit/64-bit
- Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations RS5 (October 2018 Update, 1809) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-bit/64-bit
- Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-bit/64-bit
- Microsoft Windows 10 Pro 19H1 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations 19H1 32-bit/64-bit
- Microsoft Windows 10 Enterprise 19H1 32-bit/64-bit
- Microsoft Windows 10 Education 19H1 32-bit/64-bit
- Microsoft Windows 10 Pro 19H2 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations 19H2 32-bit/64-bit
- Microsoft Windows 10 Enterprise 19H2 32-bit/64-bit
- Microsoft Windows 10 Education 19H2 32-bit/64-bit
- Microsoft Windows 8.1 Pro 32-bit/64-bit
- Microsoft Windows 8.1 Enterprise 32-bit/64-bit
- Microsoft Windows 8 Pro 32-bit/64-bit
- Microsoft Windows 8 Enterprise 32-bit/64-bit
- Microsoft Windows 7 Professional with Service Pack 1 and higher 32-bit/64-bit
- Microsoft Windows 7 Enterprise/Ultimate with Service Pack 1 and higher 32-bit/64-bit
- Windows Server 2019 Standard 64-bit
- Windows Server 2019 Core 64-bit
- Windows Server 2019 Datacenter 64-bit
- Windows Server 2016 Server Standard RS3 (v1709) (LTSC/CBB) 64-bit
- Windows Server 2016 Server Datacenter RS3 (v1709) (LTSC/CBB) 64-bit
- Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSC/CBB) 64-bit
- Windows Server 2016 Standard (LTSC) 64-bit
- Windows Server 2016 Server Core (Installation Option) (LTSC) 64-bit
- Windows Server 2016 Datacenter (LTSC) 64-bit
- Windows Server 2012 R2 Standard 64-bit
- Windows Server 2012 R2 Server Core 64-bit
- Windows Server 2012 R2 Foundation 64-bit
- Windows Server 2012 R2 Essentials 64-bit
- Windows Server 2012 R2 Datacenter 64-bit
- Windows Server 2012 Standard 64-bit
- Windows Server 2012 Server Core 64-bit
- Windows Server 2012 Foundation 64-bit
- Windows Server 2012 Essentials 64-bit
- Windows Server 2012 Datacenter 64-bit
- Windows Storage Server 2016 64-bit
- Windows Storage Server 2012 R2 64-bit
- Windows Storage Server 2012 64-bit

7.6.2. Características Generales

7.6.2.1. La solución debe disponer de una consola de gestión centralizada que

permita la instalación, configuración, actualización y administración de todas las soluciones ofertadas de manera integral, facilitando la gestión de la seguridad tanto en modalidad On-Premise como en la Nube.

7.6.2.2. Se debe acceder a la consola On-Premise vía WEB (HTTPS), MMC.

7.6.2.3. Compatibilidad con Windows Failover clustering u otra solución de alta disponibilidad en el caso de consola On-Premise.

7.6.2.4. Capacidad de eliminar remotamente cualquier solución de seguridad

(propia o de terceros) que esté presente en las estaciones y servidores, sin la necesidad de la contraseña de remoción de la actual solución de seguridad.

7.6.2.5. Capacidad de instalar remotamente la solución en las estaciones y

servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory;

7.6.2.6. Capacidad de instalar remotamente la solución de seguridad en

smartphones y tablets Android, utilizando estaciones como intermediadoras.

7.6.2.7. Capacidad de gestionar estaciones de trabajo y servidores de archivos

(tanto Windows como Linux y Mac) protegidos por la solución;

7.6.2.8. Capacidad de gestionar smartphones y tablets (tanto Android y iOS)

protegidos por la solución.

7.6.2.9. Capacidad de generar paquetes personalizados (autoejecutables)

conteniendo la licencia y configuraciones del producto.

7.6.2.10. Capacidad de actualizar los paquetes de instalación con las últimas

vacunas, para que cuando el paquete sea utilizado en una instalación ya contenga las últimas vacunas lanzadas.

7.6.2.11. Capacidad de monitorear diferentes subnets de red con el objetivo de

encontrar máquinas nuevas para que sean agregadas a la protección.

7.6.2.12. Capacidad de monitorear grupos de trabajos ya existentes y cualquier

grupo de trabajo que sea creado en la red, a fin de encontrar máquinas nuevas para ser agregadas a la protección.

7.6.2.13. Capacidad de, al detectar equipos nuevos en el Active Directory,

subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antimalware instalado. En caso de no tenerlo, debe instalar el antimalware automáticamente.

7.6.2.14. Capacidad de agrupamiento de máquinas por características comunes

entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antimalware instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 2 días, etc.

7.6.2.15. Capacidad de definir políticas de configuraciones diferentes por grupos

de estaciones, permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos.

7.6.2.16. Capacidad de importar la estructura de Active Directory para encontrar

máquinas.

7.6.2.17. Debe proporcionar las siguientes informaciones de las computadoras:

- Si el antimalware está instalado.
- Si el antimalware ha iniciado.
- Si el antimalware está actualizado.
- Minutos/horas desde la última conexión de la máquina con el servidor administrativo.
- Minutos/horas desde la última actualización de vacunas.
- Fecha y horario de la última verificación ejecutada en la máquina.
- Versión del antimalware instalado en la máquina.
- Si es necesario reiniciar la computadora para aplicar cambios.
- Fecha y horario de cuando la máquina fue encendida.
- Cantidad de virus encontrados (contador) en la máquina.
- Nombre de la computadora.
- Dominio o grupo de trabajo de la computadora.
- Fecha y horario de la última actualización de vacunas.
- Sistema operativo con Service Pack.
- Cantidad de procesadores.
- Cantidad de memoria RAM.
- Usuario(s) conectados en ese momento, con información de contacto (si están disponibles en el Active Directory).
- Dirección IP.
- Aplicativos instalados, inclusive aplicativos de terceros, con historial de instalación, conteniendo fecha y hora que el software fue instalado o removido.
- Actualizaciones de Windows Updates instaladas.
- Información completa de hardware conteniendo: procesadores, memoria, adaptadores de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD.
- Vulnerabilidades de aplicativos instalados en la máquina.

7.6.2.18. Debe permitir bloquear que el usuario cambie las configuraciones de la solución instalada en las estaciones y servidores.

7.6.2.19. Capacidad de reconectar máquinas clientes al servidor administrativo más próximo, basado en reglas de conexión como:

- Cambio de gateway.
- Cambio de subnet DNS.
- Cambio de dominio.
- Cambio de servidor DHCP.
- Cambio de servidor DNS.
- Cambio de servidor WINS.
- Aparición de nueva subnet.

- 7.6.2.20. Capacidad de configurar políticas móviles para que cuando una computadora cliente esté fuera de la estructura de protección pueda actualizarse vía internet.
- 7.6.2.21. Capacidad de instalar otros servidores administrativos para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes.
- 7.6.2.22. Capacidad de interrelacionar servidores en estructura de jerarquía para obtener informes sobre toda la estructura de endpoints.
- 7.6.2.23. Capacidad de herencia de tareas y políticas en la estructura jerárquica de servidores administrativos.
- 7.6.2.24. Capacidad de elegir cualquier computadora cliente como repositorio de vacunas y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red.
- 7.6.2.25. Capacidad de hacer de este repositorio de vacunas un gateway para conexión con el servidor de administración, para que otras máquinas que no logran conectarse directamente al servidor puedan usar este gateway para recibir y enviar informaciones al servidor administrativo.
- 7.6.3. Capacidad de exportar informes para los siguientes tipos de archivos: PDF, HTML y XML.
- 7.6.4. Capacidad de generar traps SNMP para monitoreo de eventos;
- 7.6.5. Capacidad de enviar correos electrónicos para cuentas específicas en caso de algún evento.
- 7.6.6. Debe tener documentación de la estructura del banco de datos para generación de informes a partir de herramientas específicas de consulta (Crystal Reports, por ejemplo).
- 7.6.7. Capacidad de conectar máquinas vía Wake On Lan para realización de tareas (barrido, actualización, instalación, etc.), inclusive de máquinas que estén en subnets diferentes del servidor).
- 7.6.8. Capacidad de habilitar automáticamente una política en caso de que ocurra una infección masiva en la red (basado en cantidad de malware encontrados en determinado intervalo de tiempo).
- 7.6.9. Capacidad de realizar actualización incremental de vacunas en las computadoras clientes.
- 7.6.10. Capacidad de realizar inventario de hardware de todas las máquinas clientes.
- 7.6.11. Capacidad de realizar inventario de aplicativos de todas las máquinas clientes.
- 7.6.12. Capacidad de diferenciar máquinas virtuales de máquinas físicas.
- 7.6.13. La solución debe ser capaz de integrarse con soluciones SIEM.
- 7.6.14. La solución debe poder enviar notificaciones por correo electrónico.
- 7.6.15. La solución debe tener diferentes funciones de administrador que tengan una única interfaz / tablero durante el inicio de sesión y controladas por privilegios y derechos en función de sus roles (Administrador, Revisor, Investigador, etc.).
- 7.6.15.1. Capacidad de, en caso de epidemia, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.

7.7. EDR

- El fabricante debe de estar incluido dentro del framework MITRE ATT&CK EDR de elación de soluciones EDR.
- El fabricante debe tener experiencia probada en el descubrimiento de vulnerabilidades desconocidas, APTs, campañas de ciberespionaje y malware avanzado. Para ello debe haber publicado no menos de 100 documentos sobre campañas de APT y agentes de amenazas durante el último año.

7.7.1. COMPATIBILIDAD

- Windows 7 SP1 Home / Professional / Enterprise 32-bit / 64-bit
- Windows 8.1.1 Professional / Enterprise 32-bit / 64-bit
- Windows 10 RS3 (versión 1703) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS4 (versión 1803) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS5 (versión 1809) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 RS6 (versión 1903) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 19H2 (versión 1909) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows 10 20H1 (versión 2004) Home / Professional / Education / Enterprise 32-bit / 64-bit
- Windows Server 2008 R2 Foundation / Standard / Enterprise 64-bit
- Windows Server 2012 Foundation / Standard / Enterprise 64-bit
- Windows Server 2012 R2 Foundation / Standard / Enterprise 64-bit
- Windows Server 2016 Essentials / Standard / Datacenter 64-bit
- Windows Server 2019 Essentials / Standard / Datacenter 64-bit

7.7.2. CARACTERÍSTICAS

- B*
- A*
- M*
- 7.7.2.1. La solución debe admitir la detección automatizada de actividad maliciosa mediante soluciones Endpoint Protección.
- 7.7.2.2. La solución sugerida debe complementar la información del veredicto de la solución Endpoint Protection con los artefactos del sistema sobre la detección.
- 7.7.2.3. La solución sugerida debe admitir la generación automática de indicadores de amenazas y/o compromiso (IoC) después de que se produzca la detección con la capacidad de aplicar una acción de respuesta.
- 7.7.2.4. La solución debe tener la capacidad de forzar la ejecución de un escaneo de IoC en todos los puntos finales con agentes EDR instalados.
- 7.7.2.5. La solución debe admitir la ejecución de análisis de IoC de acuerdo a una planificación indicada por el administrador o analista.
- 7.7.2.6. La solución debe admitir la importación de IoC de terceros en formato OpenIoC para su uso en el escaneo de los equipos.
- 7.7.2.7. La solución debe admitir el escaneo utilizando un conjunto de IoC generado automáticamente, cargado o externo (de terceros) para detectar amenazas no detectadas anteriormente.
- 7.7.2.8. La solución debe admitir la exportación de IoC generado por la solución a un archivo en formato OpenIoC.
- 7.7.2.9. La solución debe permitir la visibilidad detallada del incidente relacionada con la amenaza detectada en un endpoint.
- 7.7.2.10. La información detallada del incidente debe incluir al menos la siguiente información de la amenaza detectada:
- Gráfico de la cadena de desarrollo de amenazas (kill chain).
 - Información sobre el dispositivo en el que se detecta la amenaza (nombre, dirección IP, dirección MAC, lista de usuarios, sistema operativo).
 - Información general sobre la detección, incluido el modo de detección.
 - Cambios de registro asociados a la detección.
 - Historial de presencia de archivos en el dispositivo.
 - Acciones de respuesta realizadas por la aplicación.
- 7.7.2.11. El gráfico de la cadena de desarrollo de amenazas (kill chain) debe proporcionar información visual sobre los objetos involucrados en el incidente, por ejemplo, sobre procesos clave en el dispositivo, conexiones de red, bibliotecas, registro, etc.
- 7.7.2.12. La información de un incidente debe presentar una vista detallada de los artefactos del sistema y los datos relacionados con el incidente para el

análisis de la causa raíz:

- Proceso de spawning
- Conexiones de red
- Cambios en el registro
- Descarga de archivos
- Dropped de objetos

7.7.2.13. La solución debe admitir una comunicación segura entre la consola de administración y los puntos finales con el agente EDR.

7.7.2.14. La solución debe admitir la gestión del agente EDR a través de la interfaz de línea de comandos y por la consola.

7.7.2.15. La solución debe tener una función / módulo incorporado para recopilar los datos necesarios para la resolución de problemas, sin requerir un acceso físico al punto final.

7.7.2.16. El agente EDR debe tener un mecanismo de autodefensa para evitar que el agente modifique archivos relacionados con el agente / entradas de componentes del sistema, etc.

7.8. CIFRADO DE DATOS

7.8.1. COMPATIBILIDAD

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 or later.
- Windows 8 Professional / Enterprise.
- Windows 8.1 Professional / Enterprise.
- Windows 10 Home / Pro / Education / Enterprise.

7.8.2. CARACTERÍSTICAS

7.8.2.1. El acceso al recurso cifrado (archivo, carpeta o disco) debe ser garantizado aún en caso de que el usuario haya olvidado la contraseña, a través de procedimientos de recuperación.

7.8.2.2. Utilizar, como mínimo, un algoritmo AES con clave de 256 bits.

7.8.2.3. Capacidad de cifrar completamente el disco duro de la máquina, agregando un ambiente de preboot para autenticación del usuario.

7.8.2.4. Capacidad de utilizar Single Sign-On para la autenticación de preboot.

7.8.2.5. Permitir crear varios usuarios de autenticación preboot.

7.8.2.6. Capacidad de crear un usuario de autenticación preboot común con una contraseña igual para todas las máquinas a partir de la consola de manejo.

7.8.2.7. Capacidad de cifrar drives extraíbles de acuerdo con una regla creada por el administrador, con las opciones:

- Cifrar solamente los archivos nuevos que sean copiados para el disco extraíble, sin modificar los archivos ya existentes.
- Cifrar todos los archivos individualmente.
- Cifrar el dispositivo entero, de manera que no sea posible listar los archivos y carpetas almacenadas.
- Cifrar el dispositivo en modo portátil, permitiendo acceder a los archivos en máquinas de terceros a través de una contraseña.

7.8.2.8. Capacidad de seleccionar carpetas y archivos (por tipo, o extensión) para ser cifradas automáticamente. En esta modalidad, los archivos deben estar accesibles para todas las máquinas gestionadas por la misma consola de manera transparente para los usuarios.

7.8.2.9. Capacidad de crear reglas de exclusiones para que ciertos archivos o carpetas nunca sean cifrados.

7.8.2.10. Capacidad de seleccionar aplicaciones que pueden o no tener acceso a los archivos cifrados.

7.9. GESTIÓN DE SISTEMAS

7.9.1. Gestión de Vulnerabilidades. Capacidad de detectar software de Microsoft y de terceros vulnerables, creando así un informe de software vulnerable.

7.9.2. Capacidad de corregir las vulnerabilidades de software de cualquier proveedor, haciendo la descarga centralizado o descentralizado de la corrección o

- actualización y aplicando esa corrección o actualización en las máquinas gestionadas de manera transparente para los usuarios.
- 7.9.3. Permite la planificación de fecha y hora para el despliegue de parches y actualizaciones, discriminando PCs y Servidores.
 - 7.9.4. Sincronización con Microsoft Update, para el despliegue centralizado de Parches y actualizaciones Microsoft.
 - 7.9.5. Capacidad de gestionar licencias de software de terceros.
 - 7.9.6. Utilización de Puntos de distribución para el despliegue de parches y actualizaciones en entornos WAN para reducir la utilización de ancho de banda.
 - 7.9.7. Capacidad de gestionar un inventario de hardware, con la posibilidad de registro de dispositivos (ej.: router, switch, proyector, accesorio, etc.), informando fecha de compra, lugar donde se encuentra, service tag, número de identificación y otros.
 - 7.9.8. Capacidad de registro de información adicional en los activos de la empresa mediante campos personalizados.

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 PAGO¹⁰

LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en Soles, en Unico Pago, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.

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

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

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

CLÁUSULA QUINTA: DEL PLAZO DE ENTREGA

El proveedor tendrá un plazo máximo de veinte (20) días calendario, a partir de la suscripción del contrato para la implementación de las licencias de software y entrega del bien e instalación del servidor consola, el plazo será computado a partir del día siguiente de firmado el contrato y/o notificada la orden de compra, lo que ocurra primero.

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

Entregables

Una vez culminada la instalación, configuración y pruebas se suscribirá un acta de implementación, para ello el proveedor deberá entregar la siguiente documentación técnica:

- Informe técnico de implementación.
- Procedimiento de solicitud de Soporte Técnico a nivel del Proveedor y del Fabricante.

Garantía Comercial

La garantía comercial que el postor brinde entrará en vigencia a partir del inicio de la suscripción; y tendrá una duración de (24) meses.

Capacitación

- El instructor que impartirá la capacitación, deberá tener como mínimo grado profesional Técnico Titulado o Bachiller en las especialidades de: ingeniería de sistemas, informática, electrónica y/o ramas afines, acreditar documentariamente certificación del fabricante del producto de la solución ofertada, así como certificaciones y/o estudios en seguridad informática Ethical Hacking.
- Dicha capacitación se dictará en las instalaciones de la entidad y/o remoto según la coyuntura actual.
- Curso para 4 integrantes del Cenares en Alta Especialización en Gestión de TI (Itil 4 Fundam + Cobit 2019 Fund + CISSP) que consta de 101 horas lectivas e incluye Certificación.
- La capacitación podrá dictarse en un plazo posterior a la etapa de implementación y/o dentro del mismo periodo, pero será requisito para efectos de conformidad, contar con el registro del participante al curso.

Otras consideraciones adicionales:

Durante el tiempo que dure el Estado de Emergencia declarado por el Gobierno a consecuencia del COVID-19, EL CONTRATISTA deberá cumplir con las siguientes condiciones del servicio:

- a. En la entrega de los bienes, así como los trabajos y/o visitas que se realicen en las instalaciones de la Entidad para la ejecución de la prestación, el personal del proveedor deberá cumplir con los protocolos sanitarios de operación ante el COVID-19 establecidos en el "Plan de vigilancia, prevención y control de COVID-19 en el trabajo" de la Entidad y lo dispuesto en la Resolución Ministerial N° 448-2020-MINSA.
- b. Deberá proporcionar permanentemente a su personal los equipos de protección personal e implementos de limpieza y desinfección, para la provisión del servicio; debiendo brindar (como mínimo) los siguientes:
 - Equipos de protección:
 - i. Mascarillas quirúrgicas
 - ii. Guantes de látex
 - iii. Lentes de seguridad
 - Implementos de limpieza y desinfección: iv. Alcohol en gel o soluciones desinfectantes
 - v. Jabón líquido y papel o toallas desechables, para el lavado de manos de su personal
- c. Control de temperatura corporal del personal.
- d. Guardar el distanciamiento social establecido en todo momento.
- e. Presentar el Plan de Vigilancia, Prevención y Control de COVID-19, al inicio de la entrega del bien (que cuente con la aprobación por parte del Comité de Seguridad y Salud en el Trabajo o el supervisor de

Seguridad y Salud en el Trabajo de la empresa CONTRATISTA)

- f. Cumplir las instrucciones que se le den al ingresar y demás disposiciones que dicten los sectores y autoridades competentes al respecto.

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

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

CLÁUSULA SÉTIMA: GARANTÍAS

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

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

Importante

De conformidad con el artículo 152 del Reglamento, no se constituirá garantía de fiel cumplimiento del contrato ni garantía de fiel cumplimiento por prestaciones accesorias, en contratos cuyos montos sean iguales o menores a cien mil Soles (S/ 100,000.00). Dicha excepción también aplica a 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 no supere el monto señalado anteriormente.

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: CONFIDENCIALIDAD

El contratista del servicio tiene y asume la obligación, tanto durante la vigencia del contrato, como después de su extinción, de guardar el secreto y la confidencialidad de cualquier información del Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud - CENARES a la que tenga acceso como consecuencia del desempeño de su servicio, quedando expresamente prohibido revelar dicha información.

Por lo expuesto en el párrafo precedente, el proveedor del servicio no podrá:

- Difundir, transmitir o revelar información a terceros.
- Usar la información recopilada para ofrecer, promocionar o brindar información sobre productos o servicios.
- Arrendar ni vender a terceros ningún dato de identificación personal que les haya sido proporcionado por el CENARES o como consecuencia del servicio brindado.
- Invitar al usuario a tomar parte en encuestas sobre productos, servicios, noticias o eventos.

CLÁUSULA DÉCIMA: RECEPCIÓN Y CONFORMIDAD DE LA PRESTACIÓN

La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La recepción será otorgada por el Centro de Almacen y Distribucion del CENARES y la conformidad será otorgada por el Equipo de Informatica del Centro de Gestion Administrativa del Centro Nacional de Abastecimiento en Recursos Estrategicos en Salud - CENARES previa presentación de los entregables y capacitacion en el plazo máximo de Siete (7) días de producida la recepción.

De existir observaciones, LA ENTIDAD las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no menor de dos (2) ni mayor de ocho (8) días. Dependiendo de la complejidad o sofisticación de las subsanaciones a realizar el plazo para

subsana no puede ser menor de cinco (5) ni mayor de quince (15) días. Si pese al plazo otorgado, EL CONTRATISTA no cumpliera a cabalidad con la subsanación, LA ENTIDAD puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar.

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

CLÁUSULA UNDÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

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

CLÁUSULA DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

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

El plazo máximo de responsabilidad del contratista es de dos (2) 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.

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 CONTROVERSIAS¹¹

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.

¹¹ De acuerdo con el numeral 225.3 del artículo 225 del Reglamento, las partes pueden recurrir al arbitraje ad hoc cuando las controversias deriven de procedimientos de selección cuyo valor estimado sea menor o igual a cinco millones con 00/100 soles (S/ 5 000 000,00).

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: Jr Nazca N° 548 – Jesus Maria

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 triplicado en señal de conformidad en la ciudad de [.....] al [CONSIGNAR FECHA].

"LA ENTIDAD"

"EL CONTRATISTA"

ANEXOS

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° 014-2021-CENARES/MINSA

Presente.-

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

Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :	Teléfono(s) :		
MYPE ¹²		Sí	No
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 compra¹³

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.

Importante

¹² Esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/> y se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

¹³ Cuando el monto del valor estimado del procedimiento o del ítem no supere los doscientos mil Soles (S/ 200,000.00), en caso se haya optado por perfeccionar el contrato con una orden de compra.

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

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° 014-2021-CENARES/MINSA

Presente.-

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

Datos del consorciado 1				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁴		Sí	No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁵		Sí	No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁶		Sí	No	
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.

¹⁴ Esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/> y se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento. Para dicho efecto, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

¹⁵ Ibidem.

¹⁶ Ibidem.

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 compra¹⁷

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

¹⁷ Cuando el monto del valor estimado del procedimiento o del ítem no supere los doscientos mil Soles (S/ 200,000.00), en caso se haya optado por perfeccionar el contrato con una orden de compra.

ANEXO N° 2

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

Señores

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° 014-2021-CENARES/MINSA

Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

ANEXO N° 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS

Señores

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° 014-2021-CENARES/MINSA

Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del procedimiento de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece el [CONSIGNAR EL OBJETO DE LA CONVOCATORIA], 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]

B

A

1

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

Importante

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

ANEXO N° 4

DECLARACIÓN JURADA DE PLAZO DE ENTREGA

Señores

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° 014-2021-CENARES/MINSA

Presente.-

Mediante el presente, con pleno conocimiento de las condiciones que se exigen en las bases del procedimiento de la referencia, me comprometo a entregar los bienes objeto del presente procedimiento de selección en el plazo de [CONSIGNAR EL PLAZO OFERTADO. EN CASO DE LA MODALIDAD DE LLAVE EN MANO DETALLAR EL PLAZO DE ENTREGA, SU INSTALACIÓN Y PUESTA EN FUNCIONAMIENTO].

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 5

PROMESA DE CONSORCIO

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

Señores

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° 014-2021-CENARES/MINSA

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 **ADJUDICACIÓN SIMPLIFICADA N°** [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

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

a) Integrantes del consorcio

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

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

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

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

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

1. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] [%]¹⁸

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]¹⁹

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES

100%²⁰

[CONSIGNAR CIUDAD Y FECHA]

¹⁸ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

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

²⁰ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

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

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

Importante

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

B

A

M

ANEXO N° 6

PRECIO DE LA OFERTA

Señores

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° 014-2021-CENARES/MINSA

Presente.-

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

CONCEPTO	PRECIO TOTAL
TOTAL	S/

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

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

B

A

M

ANEXO N° 7

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 014-2021-CENARES/MINSA

Presente.-

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

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²¹	FECHA DE LA CONFORMIDAD DE SER EL CASO ²²	EXPERIENCIA PROVENIENTE ²³ DE:	MONEDA	IMPORTE ²⁴	TIPO DE CAMBIO VENTA ²⁵	MONTO FACTURADO ACUMULADO ²⁶
1										
2										
3										

²¹

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.

²²

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.

²³

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".

²⁴

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

²⁵

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.

²⁶

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 21	FECHA DE LA CONFORMIDAD DE SER EL CASO 22	EXPERIENCIA PROVENIENTE 23 DE:	MONEDA	IMPORTE 24	TIPO DE CAMBIO VENTA 25	MONTO FACTURADO ACUMULADO 26
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 N° 8

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

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 014-2021-CENARES/MINSA

Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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

ANEXO N° 9

SOLICITUD DE BONIFICACIÓN DEL CINCO POR CIENTO (5%) POR TENER LA CONDICIÓN DE MICRO Y PEQUEÑA EMPRESA

Señores

COMITÉ DE SELECCIÓN

ADJUDICACIÓN SIMPLIFICADA N° 014-2021-CENARES/MINSA

Presente.-

Mediante el presente el suscrito, postor y/o Representante legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], solicito la asignación de la bonificación del cinco por ciento (5%) sobre el puntaje total obtenido, debido a que mi representada cuenta con la condición de micro y pequeña empresa.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

- Para asignar la bonificación, el órgano encargado de las contrataciones o comité de selección, según corresponda, verifica la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/>.
- Para que un consorcio pueda acceder a la bonificación, cada uno de sus integrantes debe cumplir con la condición de micro y pequeña empresa.