

# BASES ESTÁNDAR DE LICITACIÓN PÚBLICA 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	Importante • Abc	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y por los proveedores.
4	Advertencia • Abc	Se refiere a advertencias a tener en cuenta por el comité de selección y por los proveedores.
5	Importante para la Entidad • Xyz	Se refiere a consideraciones importantes a tener en cuenta por el comité de selección y deben ser eliminadas una vez culminada la elaboración de las bases.

### CARACTERÍSTICAS DEL DOCUMENTO:

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

N°	Características	Parámetros
1	Márgenes	Superior : 2.5 cm Izquierda: 2.5 cm Inferior: 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 junio 2019, diciembre 2019, julio 2020 y julio 2021

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

**LICITACIÓN PÚBLICA N° 008-2021-CENARES/MINSA**

**CONTRATACIÓN DE BIENES**  
**ADQUISICIÓN DE EQUIPO DE SEGURIDAD PERIMETRAL -  
FIREWALL**

B  
W  
Q

## DEBER DE COLABORACIÓN

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

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

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

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

## **SECCIÓN GENERAL**

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

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

B  
W  
d

## CAPÍTULO I ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

### 1.1. REFERENCIAS

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

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

### 1.2. CONVOCATORIA

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

### 1.3. REGISTRO DE PARTICIPANTES

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

#### Importante

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

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

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

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

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

#### Importante



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

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

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

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

##### **Advertencia**

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

##### **Importante**

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

#### 1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

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

##### **Importante**

- *Los formularios electrónicos que se encuentran en el SEACE y que los proveedores deben llenar para presentar sus ofertas, tienen carácter de declaración jurada.*
- *En caso la información contenida en los documentos escaneados que conforman la oferta no coincida con lo declarado a través del SEACE, prevalece la información declarada en los documentos escaneados.*
- *No se tomarán en cuenta las ofertas que se presenten en físico a la Entidad.*

#### 1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

El participante presentará su oferta de manera electrónica a través del SEACE, desde las 00:01 horas hasta las 23:59 horas del día establecido para el efecto en el cronograma del

procedimiento; adjuntando el archivo digitalizado que contenga los documentos que conforman la oferta de acuerdo a lo requerido en las bases.

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

#### **Importante**

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

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

### **1.9. EVALUACIÓN DE LAS OFERTAS**

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

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

### **1.10. CALIFICACIÓN DE OFERTAS**

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

### **1.11. SUBSANACIÓN DE LAS OFERTAS**

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

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

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

### **1.12. RECHAZO DE LAS OFERTAS**

Previo al otorgamiento de la buena pro, el comité de selección revisa las ofertas económicas que cumplen los requisitos de calificación, de conformidad con lo establecido para el rechazo de ofertas, previsto en el artículo 68 del Reglamento, de ser el caso.

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

### **1.13. OTORGAMIENTO DE LA BUENA PRO**

Definida la oferta ganadora, el comité de selección otorga la buena pro, mediante su publicación en el SEACE, incluyendo el cuadro comparativo y las actas debidamente motivadas de los



resultados de la admisión, no admisión, evaluación, calificación, descalificación y el otorgamiento de la buena pro.

#### 1.14. CONSENTIMIENTO DE LA BUENA PRO

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

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

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

##### **Importante**

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

B  
W  
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 y es resuelto por el Tribunal de Contrataciones del Estado.

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

#### Importante

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

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

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

### 2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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

### CAPÍTULO III DEL CONTRATO

#### 3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

#### 3.2. GARANTÍAS

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

##### 3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

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

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

##### Importante

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

##### 3.2.3. GARANTÍA POR ADELANTO

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

#### 3.3. REQUISITOS DE LAS GARANTÍAS

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

periódicamente publica el Banco Central de Reserva del Perú.

#### **Importante**

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

#### **Advertencia**

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

*1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (<http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo>).*

*2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.*

*3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.*

*4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.*

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

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

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

### **3.4. EJECUCIÓN DE GARANTÍAS**

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

### **3.5. ADELANTOS**

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

### **3.6. PENALIDADES**

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

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

### 3.6.2. OTRAS PENALIDADES

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

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

### 3.7. INCUMPLIMIENTO DEL CONTRATO

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

### 3.8. PAGOS

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

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

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

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

#### **Advertencia**

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

### 3.9. DISPOSICIONES FINALES

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

## **SECCIÓN ESPECÍFICA**

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

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

R  
W  
D

## CAPÍTULO I GENERALIDADES

### 1.1. ENTIDAD CONVOCANTE

Nombre : Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud – CENARES  
RUC N° : 20538298485  
Domicilio legal : Jr. Nazca N° 548-Jesus Maria  
Teléfono: : 748-3030 Anexo 6114  
Correo electrónico: : mpauja@cenares.gob.pe

### 1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la Adquisición de Equipo de Seguridad Perimetral – Firewall.

N° Ítem	Descripción del Bien
1	01 NGFW de protección perimetral de acceso al internet CENARES
	01 NGFW de protección al centro de datos CENARES

### 1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante MEMORANDO N° 1449-2021-DG-CENARES-MINSA el 07 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 el plazo de entrega, planificación, instalación, configuración, funcionamiento y capacitación de cuarenta y cinco (45) días calendario, computados a partir del día siguiente de suscrito el contrato, 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, éste será entregado de forma gratuita. La entrega de las Bases podrá efectuarse de forma electrónica mediante el correo electrónico: [mpauja@cenares.gob.pe](mailto:mpauja@cenares.gob.pe), o recabarlas en la Oficina de Adquisiciones del CENARES, Jr. Nazca N° 548 – Jesús María, en el horario de 08:30 a las 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

- Ley N° 31084, Ley de Presupuesto del sector público para el año fiscal 2021.
- Ley N° 31085, Ley de equilibrio financiero del presupuesto del sector público para el año fiscal 2021.
- Decreto Legislativo N°1440. Decreto Legislativo del Sistema Nacional de Presupuesto Público.
- Decreto Supremo N° 082-2019-EF. TUO de la Ley N° 30225, Ley de Contrataciones del Estado, en adelante La Ley.
- Decreto Supremo N° 344-2018-EF. Reglamento de la Ley de Contrataciones del Estado, en adelante el Reglamento.
- Decreto Supremo N° 004-2019-JUS. TUO de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- Directivas del OSCE.
- Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y de Acceso a la Información.
- Decreto Legislativo N° 295. Código Civil.
- Resolución Directoral N° 497-2021-CENARES/MINSA - Designación de Comité de Selección.

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

B  
W  
D





## CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

### 2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

#### **Importante**

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

### 2.2. CONTENIDO DE LAS OFERTAS

La oferta contendrá, además de un índice de documentos<sup>1</sup>, la siguiente documentación:

#### 2.2.1. Documentación de presentación obligatoria

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

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

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

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

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

#### **Advertencia**

*De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE<sup>2</sup> 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)
- e) Adjuntar el link público del fabricante que verifique que los modelos propuestos no

<sup>1</sup> La omisión del índice no determina la no admisión de la oferta.

<sup>2</sup> 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/>

están en el listado ni anunciado en el sitio web del fabricante como end-of-life o end+of-support.

- f) Adjuntar el acceso a una herramienta que permita evaluar el nivel de adopción de buenas prácticas de configuración en el Next (link público).
- g) Declaración jurada de plazo de entrega. **(Anexo N° 4)**<sup>3</sup>
- h) 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)**
- i) 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 comité de selección verifica la presentación de los documentos requeridos. De no cumplir con lo requerido, la oferta se considera no admitida.*

#### 2.2.1.2. Documentos para acreditar los requisitos de calificación

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

#### Advertencia

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

### 2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

- a) Garantía de fiel cumplimiento del contrato. CARTA FIANZA
- 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.
- 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.

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

g) Documentación que acredite el perfil del personal clave:

**Un (1) Especialista en Seguridad Perimetral**

- Copia simple del título o grado de bachiller o título de técnico en una de las siguientes carreras profesionales: Ingeniería de sistemas y/o Ingeniería electrónica y/o Ingeniería de telecomunicaciones y/o carreras profesionales o técnicas afines relacionadas a tecnologías de la información. Carreras profesionales o técnicas afines: Ingeniería Electrónica y/o Telecomunicación y/o Ingeniería de Computación y/o Ingeniería en Sistemas e Informática y/o Ingeniería Informática y Sistemas y/o Ingeniería de Sistemas de Información y/o Ingeniería de Redes y Comunicaciones y/o Ingeniería Estadística e Informática y/o Administración de Redes y Comunicaciones y/o Administración y Sistemas y/o Redes y Comunicación de Datos y/o Informática y/o Computación y/o Ingeniero de Redes y/o Redes y Comunicaciones de Datos.
- Copia simple de la certificación a nivel técnica emitida por el fabricante de la solución ofertada y/o copia simple de la certificación técnica en la marca o producto ofertado.

**Un (1) Jefe de Proyecto**

- Copia simple del título profesional o grado de bachiller en una de las siguientes carreras profesionales: Ingeniería electrónica, Ingeniería de telecomunicaciones, Ingeniería de Sistemas, Ingeniería de Informática, Ingeniería Industrial, Cómputo.
- Copia de Certificación vigente en Project Management Professional (PMP) o en estudios como especialista en Gerencia de Proyectos.
- Copia simple de la certificación técnica en la marca o producto ofertado

**Advertencia**

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

**Importante**

- En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y en el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de lo contrario no podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".
- En los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados sea igual o menor a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.

**Importante**

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

<sup>4</sup> 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/>

- De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya<sup>5</sup>.
- La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.

## 2.4. PERFECCIONAMIENTO DEL CONTRATO

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

### Importante

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

## 2.5. FORMA DE PAGO

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 de Recursos Estratégicos de Salud - CENARES.

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

- Conformidad del responsable del Equipo de Informática del Centro de Gestión Administrativa del CENARES.
- Comprobante de pago.

Dicha documentación se debe presentar en Mesa de Partes del CENARES, sito en Jr. Nazca N° 548, Jesús María, en el horario de lunes a viernes de 08:30 hasta las 16:30 horas.

<sup>5</sup> Según lo previsto en la Opinión N° 009-2016/DTN.

### 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**

## ESPECIFICACIONES TÉCNICAS

### ADQUISICIÓN DE EQUIPO DE SEGURIDAD PERIMETRAL - FIREWALL.

#### 1. Objeto de la Contratación

Adquirir Equipos de Protección y Seguridad Perimetral Firewall NGFW Appliance para la seguridad perimetral del CENARES.

#### 2. Área Usuaría

Equipo de Informática del Centro de Gestión Administrativa (CGA)

#### 3. Finalidad Pública

La finalidad pública es contar con protección y seguridad perimetral a la red informática del CENARES, para que las áreas usuarias puedan desarrollar sus actividades en forma segura, logrando de esta manera atender las necesidades de información y operaciones para el abastecimiento de medicamentos que realiza el Centro Nacional de Abastecimiento de Recursos Estratégicos en Salud - CENARES.

#### 4. Alcance y Descripción del Bien

Se requiere la adquisición e implementación de un sistema de protección y seguridad perimetral Next Gen Firewall de tipo appliance, el cual debe estar compuesto por:

01 NGFW de protección perimetral de acceso al internet CENARES.

01 NGFW de protección al centro de datos CENARES.

Los equipos firewall NGFW deben estar instalados y configurados, uno de protección a los accesos del internet y otro para la protección de la red de datos del centro nacional de abastecimiento de recursos estratégicos de salud - CENARES. La marca ofertada de firewall de nueva generación debe pertenecer al Cuadrante de Líderes Gartner (en 2020, 2019, 2018, 2017) en NETWORKS FIREWALL.

#### 5. Especificaciones Técnicas Mínimas de los Equipos

Los dos equipos NGFW y el equipo de gestión y reportes, deben ser de la misma marca y con hardware y software del mismo fabricante, a fin de garantizar la compatibilidad de operación y eficiencia tecnológica requerido por CENARES. A continuación, se detalla las especificaciones requeridas

Especificaciones técnicas mínimas de los equipos:

Los dos equipos NGFW y el equipo de gestión y reportes, deben ser de la misma marca y con hardware y software del mismo fabricante, a fin de garantizar la compatibilidad de operación y eficiencia tecnológica requerido por CENARES. A continuación, se detalla las especificaciones requeridas:

5.1. NGFW de protección perimetral de acceso al internet CENARES

Debe soportar mínimamente los siguientes sistemas de seguridad:

5.1.1. Descripción

- 5.1.1.1. Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial.
- 5.1.1.2. El fabricante debe pertenecer al cuadrante de líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 5 reportes.
- 5.1.1.3. El fabricante debe estar catalogado como líder en el último informe de Forrester Wave Automated Malware Analysis.
- 5.1.1.4. El fabricante deberá tener una efectividad de seguridad mayor o igual al 97% según el último reporte de NSS Labs para Next Generation Firewall.
- 5.1.1.5. La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.
- 5.1.1.6. Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end+of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.
- 5.1.1.7. Los equipos NGFW deberán tener soporte vigente de fábrica durante la fecha de contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware de un día para otro o NBD (next business day).
- 5.1.1.8. Se deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad tendrá la potestad de dar seguimiento a los casos abiertos por el Postor.
- 5.1.1.9. Como opcional, se deberá proporcionar una cuenta de acceso al portal oficial de educación del fabricante, donde la Entidad tendrá la potestad de acceder, de manera gratuita y a demanda, a cursos en línea sobre las diversas tecnologías del fabricante, así como exámenes y certificaciones.
- 5.1.1.10. Como parte de la propuesta, se deberá proporcionar el acceso a una herramienta que permita evaluar el nivel de adopción de buenas prácticas de configuración en el Next Generation Firewall implementado, con la finalidad de mejorar la postura de seguridad de red proporcionada por la solución.
- 5.1.1.11. Dicha herramienta mínimamente deberá contemplar la adopción de buenas prácticas en materia de configuración de los diferentes módulos de seguridad de la solución, como mínimo estos: Control de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, Gestión de Logs. Se requiere

que la propuesta incluya documentación pública sobre dicha herramienta explicando su alcance.

- 5.1.1.12. La herramienta de evaluación de buenas prácticas deberá ser específica para la configuración de Next Generation Firewall implementado, no se aceptarán portales con guías de usuarios genéricas.
- 5.1.1.13. La Entidad deberá poder realizar la evaluación de buenas prácticas a libre demanda y de manera autónoma.
- 5.1.1.14. El Postor deberá ejecutar la evaluación de buenas prácticas de forma semestral con el objetivo de proporcionar un servicio de mejora continua sobre las configuraciones del Next Generation Firewall. En base a la evaluación realizada, se deberá coordinar la implementación de las configuraciones recomendadas por la herramienta, previa coordinación entre el Postor y la Entidad.
- 5.1.1.15. Como parte de la propuesta, personal del Fabricante deberá realizar una evaluación de buenas prácticas de implementación. Esta evaluación deberá validar el nivel de adopción de buenas prácticas de configuración del NGFW implementado en la Entidad: se deberá entregar un informe con las recomendaciones técnicas para mejorar la adopción de las mejores prácticas de seguridad del equipo NGFW. Esta evaluación se deberá realizar dentro de los tres primeros meses posterior a la finalización de la implementación del NGFW y previa coordinación entre la Entidad y el Postor.
- 5.1.1.16. Si se identifica actividad sospechosa y/o maliciosa en la red, o sufra una brecha de seguridad luego de implementar las buenas prácticas de seguridad sugeridas por la herramienta de evaluación, la Entidad tendrá la potestad de contar con un servicio directo con el Fabricante, el cual incluye:
- Expertos, herramientas especializadas de inteligencia de amenazas y prácticas de cacería de amenazas.
  - Análisis de logs e indicadores de compromiso
  - Evaluación de la configuración del NGFW que incluya recomendaciones personalizadas
  - Recomendaciones de pasos siguientes a realizar

5.1.2. Capacidad

- 5.1.2.1. Throughput de Next Generation Firewall de 5 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño). No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.

- 5.1.2.2. Throughput de Prevención de Amenazas de 2.4 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), Filtro de Archivos, y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el nivel o modo más alto de inspección. Se debe garantizar que el





equipo no degrade su performance por debajo de lo requerido por la Entidad cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.

- 5.1.2.3. El equipo debe soportar como mínimo 1 millón sesiones simultaneas y 50 mil sesiones por segundo, medidos con paquetes HTTP de 1 byte.
- 5.1.2.4. Raqueable en 2 RU unidades de rack como mínimo.
- 5.1.2.5. Debe contar con fuente de poder redundante con capacidad de cambio en caliente.
- 5.1.2.6. Disco de estado sólido interno de 240 GB o superior.
- 5.1.2.7. Mínimo diez (10) interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red
- 5.1.2.8. Mínimo cuatro (04) interfaces de red 1G en formato SFP para el tráfico de datos de la red
- 5.1.2.9. Mínimo cuatro (04) interfaces de red 10G en formato SFP+ para el tráfico de datos de la red
- 5.1.2.10. Como opcional la plataforma deberá contar con al menos dos (02) interfaces adicionales 10/100/1000 y una (01) interfaz 10G SFP+ dedicadas a la sincronización de estado y configuración dentro del clúster de alta disponibilidad.
- 5.1.3. Características Generales
- 5.1.3.1. El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
- 5.1.3.2. Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
- 5.1.3.3. Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPsec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones.
- 5.1.3.4. Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.
- 5.1.3.5. Permitir NAT de destino basado en dominio en lugar de IP. El equipo deberá ser capaz de balancear el tráfico entrante por esa regla de NAT de destino.
- 5.1.3.6. Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.
- 5.1.3.7. Soportar túneles GRE como punto inicio o finalización del túnel.
- 5.1.3.8. Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPsec no cifrado, sin necesidad de que el equipo de seguridad sea el punto final del túnel.
- 5.1.3.9. Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo.
- 5.1.3.10. Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales.



- 8
- 5.1.4. Funcionalidades de Firewall
- 5.1.4.1. Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos) y categorías de aplicaciones.
- 5.1.4.2. Deberá ser posible la identificación de la aplicación y la inspección de malware, spyware y exploits dentro del tráfico cifrado por los protocolos en mención.
- 5.1.4.3. Permitir el agendamiento de las políticas de seguridad.
- 5.1.4.4. Debe ser posible especificar en las reglas de seguridad un grupo de objetos basados en IP y/o URL que se alimenten dinámicamente de una fuente externa.
- 5.1.4.5. Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.
- 5.1.4.6. Permitir añadir un comentario de auditoría cada vez que se cree o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoría.
- 5.1.4.7. Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).
- 5.1.4.8. Debe mostrar la primera y última vez que se utilizó una regla de seguridad.
- 5.1.4.9. Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.
- 5.1.4.10. Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.
- 5.1.5. Descifrado de Tráfico SSL/TLS
- 5.1.5.1. Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.
- 5.1.5.2. Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.
- 5.1.5.3. Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3.
- 5.1.5.4. Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros.
- 5.1.5.5. Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS
- 5.1.5.6. Debe soportar certificados que utilice Subject Alternative Name (SAN) y Server Name Indication (SNI).
- 5.1.5.7. Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.
- 5.1.5.8. Para los certificados almacenados localmente en el firewall, tiene que ser posible bloquear la posibilidad de exportar las claves privadas, para evitar un uso indebido por parte de los administradores.
- 5.1.5.9. Debe contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL/TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo debe tener varios estados de troubleshooting y
- 5



proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del tráfico (por ejemplo, informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).

**5.1.6. Control de Aplicaciones**

- 5.1.6.1.** Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.
- 5.1.6.2.** Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2
- 5.1.6.3.** Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.
- 5.1.6.4.** Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.
- 5.1.6.5.** Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, ejemplo si 2 aplicaciones utilizan el mismo puerto y protocolo, se tienen que poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación.
- 5.1.6.6.** Debe poder identificar y crear políticas de seguridad basadas en aplicaciones de Sistemas de Infraestructura Crítica (ICS) como addp, bacnet, modbus, dnp3, coap, dlms, iccp, iec-60870-5-104, mms-ics, rockwell, siemens, entre otros.
- 5.1.6.7.** Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado.
- 5.1.6.8.** Con el objetivo de identificar aplicaciones propietarias a nivel de capa 7, la solución debe permitir nativamente la creación de aplicaciones personalizadas desde la interfaz de gestión, sin la necesidad de acción por parte del fabricante.
- 5.1.6.9.** Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en sus atributos.
- 5.1.6.10.** Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz gráfica debe sugerir y permitir agregar las aplicaciones dependientes de la seleccionada, para poder permitir el uso correcto de la política de seguridad en capa 7.
- 5.1.6.11.** Debe contar con un módulo de optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.
- 5.1.7. Protección ante Ataques de Denegación de Servicio (DoS)**
- 5.1.7.1.** Debe ser posible definir un umbral conexiones por segundo en base para proteger ante diversos tipos de Ataques Flood como SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood.
- 5.1.7.2.** Para el caso de los SYN Flood debe ser posible utilizar SYN Cookies como medidas de defensa



- 5.1.7.3. La protección contra ataques Flood deberán poder ser aplicadas a una interfaz del Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor)
- 5.1.7.4. La protección contra ataques Flood deberá permitir definir al menos 3 tipos de umbrales, el primero para generar una alerta al administrador, el segundo para activar la protección y el tercero para restringir el acceso en su totalidad en base a dicha política de DoS
- 5.1.7.5. Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep, asimismo, debe ser posible definir un umbral definido en eventos por segundo para estos tipos de escaneo
- 5.1.7.6. La protección contra ataques de escaneo deberá permitir definir una lista de excepciones basadas en direcciones IP origen, a los cuales no se le aplicarán la protección.
- 5.1.7.7. Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route
- 5.1.7.8. Debe proteger contra ataques basados en protocolos No-IP en interfaces Layer 2 (como Appletalks, Banyan, VINES, Novell, SCADA), la solución deberá soportar la definición de protocolos a ser aceptados en base al formato Ethertype (Hex).
- 5.1.7.9. Debe permitir limitar un número máximo de sesiones que podrán ser generadas hacia un equipo destino, con la finalidad de evitar la saturación de sesiones hacia dicho equipo.
- 5.1.8. Prevención de Amenazas Conocidas**
- 5.1.8.1. Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.
- 5.1.8.2. Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por spyware en entornos corporativos
- 5.1.8.3. Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.
- 5.1.8.4. El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.
- 5.1.8.5. Las firmas deberán estar basadas en patrones del malware y no únicamente en hashes, con el objetivo de detectar malware polimórfico que pertenezca a una misma familia.
- 5.1.8.6. Debe sincronizar las firmas de seguridad cuando el Firewall se implementa en alta disponibilidad.
- 5.1.8.7. Debe soportar granularidad en las políticas de IPS, Antivirus y Antispyware/Antibot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.
- 5.1.8.8. Debe permitir capturar el paquete de red (en formato PCAP) asociada a la alerta de seguridad.
- 5.1.8.9. Debe identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que el Firewall pueda bloquear dichas consultas DNS.

- 5.1.8.10. Los eventos deben identificar el país que origino la amenaza.
- 5.1.8.11. Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
- 5.1.8.12. Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención.
- 5.1.8.13. Debe soportar la creación de firmas de IPS basadas en el formato de Snort.
- 5.1.9. Análisis de Malware de Día Cero**
- 5.1.9.1. La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.
- 5.1.9.2. La plataforma de Sandboxing deberá tener capacidades robustas que cumplan con altos niveles de ciberseguridad para la detección de amenazas de día cero.
- 5.1.9.3. La plataforma de Sandboxing debe ser ofrecido en Nube (Cloud). Como mínimo se requiere que el Sandbox propuesto pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y Mac.
- 5.1.9.4. El Next Generation Firewall debe tener capacidad de enviar 100 archivos por minuto al Sandbox Cloud.
- 5.1.9.5. Deberá emular los archivos sospechosos en entornos Windows, Linux, Android y Mac sin estar limitado a una capacidad de hardware ni VMs (Virtual Machines)
- 5.1.9.6. Deberá tener una disponibilidad del servicio de al menos 99.9% contabilizados mensualmente.
- 5.1.9.7. Deberá ser un servicio propio del fabricante, no se aceptarán plataformas que tercericen el servicio de Sandboxing con entidades tercera.
- 5.1.9.8. Deberá garantizar la privacidad y seguridad del contenido de los archivos analizados, para lo cual se requiere que cuente como mínimo con certificaciones SOC2 de AICPA, FedRAMP.
- 5.1.9.9. Deberá contar con una acreditación de una entidad tercera al fabricante de las soluciones propuestas, que certifique el alineamiento de los controles de seguridad del servicio nube a los estándares HIPAA (Health Insurance Portability and Accountability Act), GDPR (General Data Protection Regulation) y PCI (Payment Card Industry Data Security Standard)
- 5.1.9.10. El malware de día cero deberá poder ser identificado dentro de la infraestructura de la Entidad, sin necesidad de enviar el archivo a ser analizado fuera de la red.
- 5.1.9.11. Debe analizar Links/URLs para determinar si es o no malicioso, a pesar de no estar categorizada dentro de la Base de Datos del fabricante.
- 5.1.9.12. Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
- 5.1.9.13. El Next Generation Firewall debe ser capaz de enviar al sandbox de manera automática los archivos sospechosos que se propaguen por los protocolos HTTP, HTTPS, HTTP/2, FTP, SMTP, POP3, IMAP y SMB (versiones 1, 2 y 3). Tanto en IPv4 como en IPv6.



- 5.1.9.14. Debe permitir al administrador la descarga del archivo original analizado por el Sandbox.
- 5.1.9.15. Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración.
- 5.1.9.16. Deberá soportar el análisis de archivos ejecutables (EXE), DLLs, ELF (Linux), archivos comprimidos (ZIP, 7ZIP, RAR) archivos office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), archivos de tipos script (.vbs, .ps1, .js), email link, flash, archivos de MacOS (mach-o, dmg, pkg) y Android APKs en el ambiente controlado.
- 5.1.9.17. Permitir la subida de archivos al sandbox de forma manual y vía API.
- 5.1.9.18. Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
- 5.1.9.19. La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.
- 5.1.10. Filtro de Contenido Web**
- 5.1.10.1. Permite especificar la política por tiempo, horario o determinado periodo (día, mes, año, día de la semana y hora)
- 5.1.10.2. Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía Active Directory, LDAP en general y base de datos local.
- 5.1.10.3. Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs
- 5.1.10.4. Debe poseer al menos 70 categorías de URLs, incluyendo las de malware y phishing.
- 5.1.10.5. Debe permitir la creación de categorías personalizadas.
- 5.1.10.6. Debe contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas.
- 5.1.10.7. Debe identificar y categorizar los dominios nuevos, menores a 30 días de antigüedad.
- 5.1.10.8. Debe permitir la customización de la página de bloqueo.
- 5.1.10.9. Permitir la inserción o modificación de valores en la cabecera HTTP del tráfico de aplicaciones SaaS que pasen por el equipo de seguridad.
- 5.1.10.10. Debe permitir notificar al usuario, mostrándole solo una página de alerta, pero permitiéndole continuar la navegación al site.
- 5.1.10.11. Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de phishing.
- 5.1.11. Identificación de Usuarios**
- 5.1.11.1. Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, E- Novell Directory, Exchange y base de datos local.



- g
- 5.1.11.2. Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.
- 5.1.11.3. Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI.
- 5.1.11.4. Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM.
- 5.1.11.5. Debe soportar la recepción de eventos de autenticación de Controladores Wireless con 802.1x, Soluciones NAC y Proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API para la identificación de direcciones IP y usuarios.
- 5.1.11.6. Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.
- 5.1.11.7. Debe permitir la definición de grupos dinámicos de usuarios.
- 5.1.12. **Filtro De Datos**
- 5.1.12.1. Los archivos deben ser identificados por extensión y firmas.
- 5.1.12.2. Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, PE, APK, Flash, DLL, BAT, CAB, PIF, REG, archivos comprimidos en RAR, ZIP u otro) identificados sobre aplicaciones.
- 5.1.12.3. Permitir identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo, incluyendo, más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos vía expresión regular.
- 5.1.13. **VPN**
- 5.1.13.1. Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPsec o SSL.
- 5.1.13.2. La VPN IPsec debe soportar como mínimo:
- DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)
  - Autenticación MD5, SHA-1, SHA-2;
  - Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
  - Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
- 5.1.13.3. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.
- 5.1.13.4. Las VPN client-to-site deben poder operar usando el protocolo IPsec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo.
- 5.1.13.5. Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).
- 5.1.13.6. Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
- 5.1.13.7. Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN.
- 5.1.13.8. El Split Tunnel debe permitir elegir el tipo tráfico que se enrutará por el túnel VPN, basado en el nombre de la Aplicación y Dominio. Por ejemplo, la navegación a Salesforce que viaje por el túnel VPN, pero no todo el resto de tráfico de internet.
- W
- D
- 29

- 5.1.13.9. Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
- Antes del usuario se autentique en la estación;
  - Después de la autenticación del usuario en la estación usando Single Sign On (SSO);
  - Bajo demanda del usuario;
- 5.1.13.10. El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X, Linux, Android y iPhone.
- 5.1.13.11. Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.
- 5.1.13.12. La plataforma debe ser capaz de colocar en cuarentena equipos con actividad maliciosa identificada. La identificación de equipos colocados en cuarentena se debe basar en un ID inmutable del Cliente VPN, de tal forma que la restricción no pueda ser eludida (por ejemplo, si la cuarentena se hace a una IP, el malware puede modificar la IP del equipo para eludir la cuarentena)
- 5.1.13.13. Debe ser posible colocar equipos en cuarentena de forma manual o automática.
- 5.1.13.14. Debe ser posible bloquear el acceso a red de los equipos colocados en cuarentena.
- 5.1.13.15. Debe permitir la conexión a la VPN sin necesidad de instalar el agente (clientless).
- 5.1.13.16. Debe permitir configurar una postura de seguridad del equipo con el cliente VPN instalado, que permita validar ciertas características del equipo para controlar el acceso a la red, por lo menos se deberá recopilar las siguientes características: sistema operativo, dominio de red, versión de parche, software antivirus, software DLP y software de cifrado de disco. De tal forma que, si el equipo no cumple cierta condición basado en esas características, no permita el acceso a la VPN o le otorgue acceso de mayores restricciones.
- 5.1.13.17. El perfilamiento y postura mencionado en el punto anterior tiene que poder efectuarse inclusive dentro de la red interna, entre dos o más segmentos de red que controle el firewall.
- 5.1.14. **Consola de administración y monitoreo**
- 5.1.14.1. Con la finalidad de no degradar el performance de procesamiento de red y seguridad del Next Generation Firewall, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU, Memoria RAM y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante
- 5.1.14.2. Permitir exportar las reglas de seguridad en formato CSV y PDF
- 5.1.14.3. Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.
- 5.1.14.4. Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.
- 5.1.14.5. Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino)





- 5.1.14.6. Ante escenarios donde existan dos o más administradores del Next Generation Firewall logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.
- 5.1.14.7. Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política.
- 5.1.14.8. Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules).
- 5.1.14.9. Debe permitir el almacenamiento de diferentes versiones de archivos de respaldo de configuración (backup).
- 5.1.14.10. Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.
- 5.1.14.11. Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP).
- 5.1.14.12. Debe permitir la generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizo, su IP y el horario de la alteración;
- 5.1.14.13. Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoría de configuraciones, eventos de sistema.
- 5.1.14.14. Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispymware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
- 5.1.14.15. La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML.

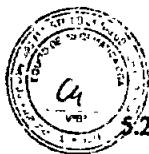
## 5.2. NGFW de protección al centro de datos CENARES

Debe soportar mínimamente los siguientes sistemas de seguridad:

- 5.2.1. Descripción
- 5.2.1.1. Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial.
- 5.2.1.2. El fabricante debe pertenecer al cuadrante de líderes de Gartner para "Enterprise Network Firewall" o "Firewalls de Redes Empresariales" en los últimos 5 reportes.
- 5.2.1.3. El fabricante debe estar catalogado como líder en el último informe de Forrester Wave Automated Malware Analysis.
- 5.2.1.4. El fabricante deberá tener una efectividad de seguridad mayor o igual al 97% según el último reporte de NSS Labs para Next Generation Firewall.



- 5.2.1.5. La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.
- 5.2.1.6. Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados ni anunciado en el sitio web del fabricante como end-of-life o end-of-sale o end-of-support. Se deberá adjuntar el link público del fabricante que verifique que los modelos propuestos no están en ese listado.
- 5.2.1.7. Los equipos NGFW deberán tener soporte vigente de fábrica durante la fecha de contrato del servicio, el soporte del fabricante deberá incluir atención de incidentes de software o hardware de la plataforma, reposición de partes o equipo de reemplazo en caso de falla de hardware de un día para otro o NBD (next business day).
- 5.2.1.8. Se deberá proporcionar una cuenta de acceso al portal oficial de soporte del fabricante, donde la Entidad tendrá la potestad de dar seguimiento a los casos abiertos por el Postor.
- 5.2.1.9. Se deberá proporcionar una cuenta de acceso al portal oficial de educación del fabricante, donde la Entidad tendrá la potestad de acceder, de manera gratuita y a demanda, a cursos en línea sobre las diversas tecnologías del fabricante, así como exámenes y certificaciones.
- 5.2.1.10. Como parte de la propuesta, se deberá proporcionar el acceso a una herramienta que permita evaluar el nivel de adopción de buenas prácticas de configuración en el Next Generation Firewall implementado, con la finalidad de mejorar la postura de seguridad de red proporcionada por la solución.
- 5.2.1.11. Dicha herramienta mínimamente deberá contemplar la adopción de buenas prácticas en materia de configuración de los diferentes módulos de seguridad de la solución, como mínimo estos: Control de Aplicaciones, Antivirus/Antimalware, Antispyware/Antibot, IPS, Sandboxing, Filtro Web, Gestión de Logs. Se requiere que la propuesta incluya documentación pública sobre dicha herramienta explicando su alcance.
- 5.2.1.12. La herramienta de evaluación de buenas prácticas deberá ser específica para la configuración de Next Generation Firewall implementado, no se aceptarán portales con guías de usuarios genéricas.
- 5.2.1.13. La Entidad deberá poder realizar la evaluación de buenas prácticas a libre demanda y de manera autónoma.
- 5.2.1.14. El Postor deberá ejecutar la evaluación de buenas prácticas de forma semestral con el objetivo de proporcionar un servicio de mejora continua sobre las configuraciones del Next Generation Firewall. En base a la evaluación realizada, se deberá coordinar la implementación de las configuraciones recomendadas por la herramienta, previa coordinación entre el Postor y la Entidad.
- 5.2.1.15. Como parte de la propuesta, personal del Fabricante deberá realizar una evaluación de buenas prácticas de implementación. Esta evaluación deberá validar el nivel de adopción de buenas prácticas de configuración del NGFW implementado en la Entidad; se deberá entregar un informe con las recomendaciones técnicas para mejorar la adopción de las mejores prácticas de seguridad del equipo NGFW. Esta evaluación se deberá realizar dentro de los tres primeros meses posterior a la finalización de la implementación del NGFW y previa coordinación entre la Entidad y el Postor.



5.2.1.16. Si se identifica actividad sospechosa y/o maliciosa en la red, o sufra una brecha de seguridad luego de implementar las buenas prácticas de seguridad sugeridas por la herramienta de evaluación, la Entidad tendrá la potestad de contar con un servicio directo con el Fabricante, el cual incluye:

- Expertos, herramientas especializadas de inteligencia de amenazas y prácticas de cacería de amenazas.
- Análisis de logs e indicadores de compromiso
- Evaluación de la configuración del NGFW que incluya recomendaciones personalizadas
- Recomendaciones de pasos siguientes a realizar

5.2.2. Capacidad

5.2.2.1. Throughput de Next Generation Firewall de 10 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño). No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.

5.2.2.2. Throughput de Prevención de Amenazas de 4.2 Gbps medido con tráfico productivo real (transacciones usando una mixtura de aplicaciones de capa 7, transacciones medidas en condiciones empresariales o transacciones HTTP 64KB de tamaño), con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, Sistema de Prevención de Intrusos (IPS), Antivirus/Antimalware de red, Antispyware/AntiBot, control de amenazas avanzadas de día cero (Sandboxing), Filtro de Archivos, y Logging activo. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el nivel o modo más alto de inspección. Se debe garantizar que el equipo no degrade su performance por debajo de lo requerido por la Entidad cuando se vayan habilitando los módulos de seguridad indicados en el modo más alto de inspección. No se aceptarán mediciones hechas con tráfico UDP o RFCs 3511, 2544, 2647 o 1242 o mixes de tráfico que no especifiquen tamaño de transacciones o paquetes.

5.2.2.3. El equipo debe soportar como mínimo 1 millón sesiones simultaneas y 50 mil sesiones por segundo, medidos con paquetes HTTP de 1 byte.

5.2.2.4. Raqueable en 2 RU unidades de rack como mínimo.

5.2.2.5. Debe contar con fuente de poder redundante con capacidad de cambio en caliente.

5.2.2.6. Disco de estado sólido interno de 240 GB o superior.

5.2.2.7. Mínimo diez (10) interfaces de red 10/100/1000 en cobre, formato RJ45 para tráfico de datos de la red

5.2.2.8. Mínimo ocho (08) interfaces de red 1G/10G en formato SFP/SFP+ para el tráfico de datos de la red

5.2.2.9. Mínimo cuatro (04) interfaces de red 40G en formato QSFP+ para el tráfico de datos de la red

5.2.2.10. Como opcional la plataforma deberá contar con al menos dos (02) interfaces adicionales 10/100/1000 y una (01) interfaz 10G SFP+ dedicadas a la sincronización de estado y configuración dentro del clúster de alta disponibilidad.



5.2.3. Características Generales

- 5.2.3.1. El dispositivo de seguridad debe soportar VLAN Tags 802.1q, agregación de links 802.3ad, policy based routing o policy based forwarding, ruteo multicast, jumbo frames, sub-interfaces ethernet lógicas, NAT de origen y destino.
- 5.2.3.2. Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
- 5.2.3.3. Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Descifrado SSL/TLS y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), OSPFv3, QoS, DHCPv6 Relay, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones.
- 5.2.3.4. Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.
- 5.2.3.5. Permitir NAT de destino basado en dominio en lugar de IP. El equipo deberá ser capaz de balancear el tráfico entrante por esa regla de NAT de destino.
- 5.2.3.6. Soportar DNS Dinámico en las interfaces de red del equipo de seguridad.
- 5.2.3.7. Soportar túneles GRE como punto inicio o finalización del túnel.
- 5.2.3.8. Capacidad de inspeccionar el contenido en túneles GRE, GPRS, VXLAN e IPSec no cifrado, sin necesidad de que el equipo de seguridad sea el punto final del túnel.
- 5.2.3.9. Soportar IPv6 en modos de alta disponibilidad, tanto Activo/Activo como Activo/Pasivo.
- 5.2.3.10. Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales.

5.2.4. Funcionalidades de Firewall

- 5.2.4.1. Control de políticas por zonas, puertos, direcciones IP, segmentos y/o rangos de red, región geográfica, usuarios y grupos de usuarios, aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en sus atributos) y categorías de aplicaciones.
- 5.2.4.2. Deberá ser posible la identificación de la aplicación y la inspección de malware, spyware y exploits dentro del tráfico cifrado por los protocolos en mención.
- 5.2.4.3. Permitir el agendamiento de las políticas de seguridad.
- 5.2.4.4. Debe ser posible especificar en las reglas de seguridad un grupo de objetos basados en IP y/o URL que se alimenten dinámicamente de una fuente externa.
- 5.2.4.5. Permitir agrupar las políticas de seguridad utilizando etiquetas u otro método.
- 5.2.4.6. Permitir añadir un comentario de auditoría cada vez que se cree o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoría.
- 5.2.4.7. Debe permitir realizar validaciones de la configuración antes de ser aplicada o instalada, esto implica, entre otras cosas, identificar y notificar cuando existan reglas generales superpuestas sobre otras específicas (shadowed rules).
- 5.2.4.8. Debe mostrar la primera y última vez que se utilizó una regla de seguridad.
- 5.2.4.9. Debe mostrar la fecha de creación y última fecha de modificación de la regla de seguridad.

5.2.4.10. Debe mostrar a través de un filtro, las reglas de seguridad que no han tenido uso en la red desde el último encendido del dispositivo firewall.

**5.2.5. Descifrado de Tráfico SSL/TLS**

5.2.5.1. Debe permitir descifrar el tráfico de navegación de usuarios a internet mediante la instalación de un certificado digital en los equipos.

5.2.5.2. Debe permitir descifrar el tráfico entrante hacia servidores HTTPS publicados en internet importando el certificado del servidor en el Firewall.

5.2.5.3. Debe ser capaz de inspección el tráfico cifrado, incluyendo el protocolo TLS 1.3.

5.2.5.4. Debe tener la capacidad de bloquear la conexión hacia sitios web cifrados con protocolos obsoletos e inseguros.

5.2.5.5. Debe identificar y notificar al cliente si está visitando una página web con certificado digital no válido o emisor no confiable, a pesar de no aplicar descifrado al tráfico SSL/TLS

5.2.5.6. Debe soportar certificados que utilice Subject Alternative Name (SAN) y Server Name Indication (SNI).

5.2.5.7. Debe permitir excluir sitios a los cuales no se les aplicará la política de descifrado, identificados por dominios y wildcards.

5.2.5.8. Para los certificados almacenados localmente en el firewall, tiene que ser posible bloquear la posibilidad de exportar las claves privadas, para evitar un uso indebido por parte de los administradores.

5.2.5.9. Debe contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL/TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo debe tener varios estados de troubleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del tráfico (por ejemplo, informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).

**5.2.6. Control de Aplicaciones**

5.2.6.1. Reconocer por lo menos 3000 aplicaciones diferentes, incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, email.

5.2.6.2. Debe procesar e inspeccionar aplicaciones que utilicen HTTP/2

5.2.6.3. Para tráfico cifrado (SSL/TLS), debe permitir el descifrado de paquetes con el fin de permitir la lectura del payload de la aplicación cifrada.

5.2.6.4. Debe inspeccionar el payload del paquete de datos con el objetivo de detectar las aplicaciones en capa 7, a través de expresiones regulares, firmas u otro mecanismo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, por ejemplo, RDP en el puerto 80 en vez del 3389.

5.2.6.5. Las políticas de seguridad deberán poder definirse 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, ejemplo si 2 aplicaciones utilizan el mismo puerto y protocolo, se tienen que poder crear 2 políticas de seguridad en las cuales se apliquen controles diferentes a cada aplicación.



- 5.2.6.6. Debe poder identificar y crear políticas de seguridad basadas en aplicaciones de Sistemas de Infraestructura Crítica (ICS) como addp, bacnet, modbus, dnp3, coap, dlms, iccp, iec-60870-5-104, mms-ics, rockwell, siemens, entre otros.
- 5.2.6.7. Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis de comportamiento del tráfico observado.
- 5.2.6.8. Con el objetivo de identificar aplicaciones propietarias a nivel de capa 7, la solución debe permitir nativamente la creación de aplicaciones personalizadas desde la interfaz de gestión, sin la necesidad de acción por parte del fabricante.
- 5.2.6.9. Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en sus atributos.
- 5.2.6.10. Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz gráfica debe sugerir y permitir agregar las aplicaciones dependientes de la seleccionada, para poder permitir el uso correcto de la política de seguridad en capa 7.
- 5.2.6.11. Debe contar con un módulo de optimización de políticas, que identifique las aplicaciones que han pasado sobre políticas basadas en puertos o de Capa 4, indicando consumo en Bytes, Hits y Fechas de visualización. Este módulo deberá facilitar la migración de la política de Capa 4 a una política de Capa 7 a través de un wizard.
- 5.2.7. **Protección ante Ataques de Denegación de Servicio (DoS)**
- 5.2.7.1. Debe ser posible definir un umbral conexiones por segundo en base para proteger ante diversos tipos de Ataques Flood como SYN Flood, UDP Flood, ICMP Flood, ICMPv6 Flood.
- 5.2.7.2. Para el caso de los SYN Flood debe ser posible utilizar SYN Cookies como medidas de defensa
- 5.2.7.3. La protección contra ataques Flood deberán poder ser aplicadas a una interfaz del Firewall o individualmente a uno o más equipos protegidos (por ejemplo, un servidor)
- 5.2.7.4. La protección contra ataques Flood deberá permitir definir al menos 3 tipos de umbrales, el primero para generar una alerta al administrador, el segundo para activar la protección y el tercero para restringir el acceso en su totalidad en base a dicha política de DoS
- 5.2.7.5. Debe identificar y bloquear ataques de escaneo de puertos TCP, UDP y Host Sweep, asimismo, debe ser posible definir un umbral definido en eventos por segundo para estos tipos de escaneo
- 5.2.7.6. La protección contra ataques de escaneo deberá permitir definir una lista de excepciones basadas en direcciones IP origen, a los cuales no se le aplicarán la protección.
- 5.2.7.7. Debe proteger contra ataques basado en paquetes IP, como mínimo IP Spoofing, Paquetes Fragmentados, Strict Source Routing, Loose Source Routing, Record Route
- 5.2.7.8. Debe proteger contra ataques basados en protocolos No-IP en interfaces Layer 2 (como Appletalks, Banyan, VINES, Novell, SCADA), la solución deberá soportar la definición de protocolos a ser aceptados en base al formato Ethertype (Hex).



5.2.7.9. Debe permitir limitar un número máximo de sesiones que podrán ser generadas hacia un equipo destino, con la finalidad de evitar la saturación de sesiones hacia dicho equipo.

**5.2.8. Prevención de Amenazas Conocidas**

5.2.8.1. Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.

5.2.8.2. Capacidad de realizar DNS Sinkhole para la identificación de equipos comprometidos por spyware en entornos corporativos

5.2.8.3. Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.

5.2.8.4. El equipo deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.

5.2.8.5. Las firmas deberán estar basadas en patrones del malware y no únicamente en hashes, con el objetivo de detectar malware polimórfico que pertenezca a una misma familia.

5.2.8.6. Debe sincronizar las firmas de seguridad cuando el Firewall se implementa en alta disponibilidad.

5.2.8.7. Debe soportar granularidad en las políticas de IPS, Antivirus y Antispyware/Antibot, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio, usuario y grupo de usuarios y la combinación de todos esos ítems.

5.2.8.8. Debe permitir capturar el paquete de red (en formato PCAP) asociada a la alerta de seguridad.

5.2.8.9. Debe identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que el Firewall pueda bloquear dichas consultas DNS.

5.2.8.10. Los eventos deben identificar el país que origina la amenaza.

5.2.8.11. Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.

5.2.8.12. Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención.

5.2.8.13. Debe soportar la creación de firmas de IPS basadas en el formato de Snort.

**5.2.9. Identificación de Usuarios**

5.2.9.1. Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de usuarios y/o grupos de usuarios a través de la integración de servicios de autenticación vía LDAP, Active Directory, E- Novell Directory, Exchange y base de datos local.

5.2.9.2. Debe poseer integración con Microsoft AD Domain Controller para la identificación de direcciones IP y usuarios. Esta integración se podrá realizar con o sin software agente.



- 5.2.9.3. Debe poder identificar la IP y el usuario de Dominio en base a Event Viewer y WMI.
- 5.2.9.4. Debe poder monitorear eventos de login y logout del Active Directory utilizando el protocolo WinRM.
- 5.2.9.5. Debe soportar la recepción de eventos de autenticación de Controladores Wireless con 802.1x, Soluciones NAC y Proxy, vía Syslog, XFF (X-forward-for) en la cabecera HTTP y/o XML API para la identificación de direcciones IP y usuarios.
- 5.2.9.6. Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal). Adicionalmente se podrá añadir un segundo factor de autenticación.
- 5.2.9.7. Debe permitir la definición de grupos dinámicos de usuarios.
- 5.2.10. Filtro De Datos**
- 5.2.10.1. Los archivos deben ser identificados por extensión y firmas.
- 5.2.10.2. Permite identificar y opcionalmente prevenir la transferencia (subida o bajada) de varios tipos de archivos (incluidos MS Office, PDF, PE, APK, Flash, DLL, BAT, CAB, PIF, REG, archivos comprimidos en RAR, ZIP u otro) identificados sobre aplicaciones.
- 5.2.10.3. Permitir identificar y opcionalmente prevenir la transferencia de información sensible basados en el contenido del archivo, incluyendo, más no limitando al número de tarjetas de crédito; y permitiendo la creación de nuevos tipos de datos vía expresión regular.
- 5.2.11. VPN**
- 5.2.11.1. Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL.
- 5.2.11.2. La VPN IPSec debe soportar como mínimo:
- DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)
  - Autenticación MD5, SHA-1, SHA-2;
  - Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
  - Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
- 5.2.11.3. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.
- 5.2.11.4. Las VPN client-to-site deben poder operar usando el protocolo IPSec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo.
- 5.2.11.5. Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).
- 5.2.11.6. Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.
- 5.2.11.7. Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN.
- 5.2.11.8. El Split Tunnel debe permitir elegir el tipo tráfico que se enrutará por el túnel VPN, basado en el nombre de la Aplicación y Dominio. Por ejemplo, la navegación a Salesforce que viaje por el túnel VPN, pero no todo el resto de tráfico de internet.
- 5.2.11.9. Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
- Antes del usuario se autentique en la estación;



- Después de la autenticación del usuario en la estación usando Single Sign On (SSO);
  - Bajo demanda del usuario;
- 5.2.11.10. El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X, Linux, Android y iPhone.
- 5.2.11.11. Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.
- 5.2.11.12. La plataforma debe ser capaz de colocar en cuarentena equipos con actividad maliciosa identificada. La identificación de equipos colocados en cuarentena se debe basar en un ID inmutable del Cliente VPN, de tal forma que la restricción no pueda ser eludida (por ejemplo, si la cuarentena se hace a una IP, el malware puede modificar la IP del equipo para eludir la cuarentena)
- 5.2.11.13. Debe ser posible colocar equipos en cuarentena de forma manual o automática.
- 5.2.11.14. Debe ser posible bloquear el acceso a red de los equipos colocados en cuarentena.
- 5.2.11.15. Debe permitir la conexión a la VPN sin necesidad de instalar el agente (clientless).
- 5.2.11.16. Debe permitir configurar una postura de seguridad del equipo con el cliente VPN instalado, que permita validar ciertas características del equipo para controlar el acceso a la red, por lo menos se deberá recopilar las siguientes características: sistema operativo, dominio de red, versión de parche, software antivirus, software DLP y software de cifrado de disco. De tal forma que, si el equipo no cumple cierta condición basado en esas características, no permita el acceso a la VPN o le otorgue acceso de mayores restricciones.
- 5.2.11.17. El perfilamiento y postura mencionado en el punto anterior tiene que poder efectuarse inclusive dentro de la red interna, entre dos o más segmentos de red que controle el firewall.
- 5.2.12. Consola de administración y monitoreo**
- 5.2.12.1. Con la finalidad de no degradar el performance de procesamiento de red y seguridad del Next Generation Firewall, la administración del equipo, gestión de reportes y gestión de logs deben contar con recursos dedicados de CPU, Memoria RAM y Disco Duro, ya sea integrado dentro del mismo appliance u otro appliance independiente del mismo fabricante
- 5.2.12.2. Permitir exportar las reglas de seguridad en formato CSV y PDF
- 5.2.12.3. Debe contar con un dashboard interactivo y gráfico que permita monitorear el uso de las aplicaciones en capa 7, sitios web visitados, actividad de los usuarios, actividad por IP (origen y destino), países origen y destino del tráfico, uso de las reglas de seguridad, actividad del tráfico malicioso, actividad de los usuarios VPN. Esta información podrá ser vista en base a Bytes y Sesiones, y ser filtrado en base a un rango de tiempo, IP, usuario, país y regla de seguridad.
- 5.2.12.4. Debe permitir el control de acceso a la gestión del equipo a través de roles personalizables.
- 5.2.12.5. Debe permitir la captura de paquetes en formato PCAP para poder ser leídos por una herramienta tercera. La captura de paquetes deberá poder ser filtrada antes del proceso de ejecución en base a la interfaz, IP y Puerto (origen y destino)



- 5.2.12.6. Ante escenarios donde existan dos o más administradores del Next Generation Firewall logueados y realizando cambios en simultáneo en la consola de gestión, la solución deberá de ser capaz de solo aplicar los cambios realizados por cada administrador individual, sin afectar o sobrescribir los cambios del otro administrador.
- 5.2.12.7. Contar con un módulo que permita comparar y que indique específicamente que cambio se hizo a una política de seguridad respecto a una versión anterior de dicha política.
- 5.2.12.8. Debe ser capaz de detectar errores humanos de configuración de reglas de seguridad donde se sobrepongan reglas generales sobre reglas específicas (shadowing rules).
- 5.2.12.9. Debe permitir el almacenamiento de diferentes versiones de archivos de respaldo de configuración (backup).
- 5.2.12.10. Debe poder realizar una copia de seguridad (backup) automática de las configuraciones y rollback de configuración a la última configuración salvada.
- 5.2.12.11. Debe permitir el monitoreo de eventos basados en SNMP, integración con SIEM a través de Syslog, y envío de alertas por correo electrónico (integrándose a un servidor SMTP).
- 5.2.12.12. Debe permitir la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo, su IP y el horario de la alteración;
- 5.2.12.13. Debe permitir la asignación de una cuota de uso de disco para definir una capacidad máxima de almacenamiento de logs de tráfico de datos, amenazas, auditoria de configuraciones, eventos de sistema.
- 5.2.12.14. Debe soportar la personalización de reportes, permitiendo mostrar información de eventos de antivirus, antispyware, IPS, navegación a internet, aplicaciones, malware de día cero, debe permitir seleccionar las columnas a mostrar, filtrar la información en base a usuarios, grupos de usuarios, direcciones IP, el rango de fechas de los datos, deben poder ser exportados en PDF y enviados automáticamente vía correo electrónico.
- 5.2.12.15. La plataforma de seguridad debe permitir realizar tareas de gestión a través del API basado en XML.
- 5.2.13. Administración y gestión del ancho de banda**
- 5.2.13.1. Con la finalidad de no degradar el performance de procesamiento de red y seguridad del Next Generation Firewall, se deberá considerar un módulo de administrador de ancho de banda que puede estar incluido dentro del equipo de seguridad o ser una solución externa. Esta solución deberá cumplir las siguientes características
- 5.2.13.2. Deberá contar con al menos 3,000 aplicaciones identificadas.
- 5.2.13.3. El equipo deberá contar con 8 procesadores, 16GB de memoria RAM y disco duro de 500GB.
- 5.2.13.4. Se debe de considerar 2 bridges, es decir 4 puertos RJ45 (10/100/1000), con bypass interno que impida la interrupción ante eventos de falla por energía del equipo.
- 5.2.13.5. Deberá estar licenciado para poder gestionar 500 Mbps de throughput simétrico inicialmente con capacidad de poder incrementar (con licenciamiento adicional) a 2 Gbps por lo menos.



- 5.2.13.6. Deberá soportar como mínimo 2 millón de flujos concurrentes.
- 5.2.13.7. Deberá soportar como mínimo 300 mil paquetes por segundo.
- 5.2.13.8. La solución deberá proveer la funcionalidad de Calidad de Servicio (QoS) para proteger el ancho de banda de aplicaciones críticas y contener el tráfico no deseado tanto en IPv4 e IPv6.
- 5.2.13.9. Las políticas o reglas de control de ancho de banda deben permitir: priorización de tráfico, definir un mínimo ancho de banda garantizado y un máximo de ancho de banda permitido.
- 5.2.13.10. Deberá contar con la funcionalidad de distribución de tráfico equitativo, la cual reparte el ancho banda por igual entre todos los dispositivos conectados. Este cálculo de repartición se realiza de forma dinámica constantemente, no es un valor estático y podrá ejecutarse para el tráfico excedente luego de que se haya priorizado las aplicaciones críticas de la Entidad.
- 5.2.13.11. Posibilidad de crear múltiples políticas de control independientes entre si, para las distintas áreas de la Entidad
- 5.2.13.12. Deberá soportar la creación de políticas basadas en tiempo. Los periodos se pueden configurar de acuerdo a las necesidades de la Entidad.
- 5.2.13.13. La solución deberá integrarse con mínimamente 4 Directorios Activos (AD) de la Entidad con la finalidad de manejar políticas basadas en usuarios.
- 5.2.13.14. Permitir la creación de aplicaciones personalizadas de la propia Entidad para su visibilidad y control. Estas aplicaciones se podrán crear a través de IP y/o puerto y/o url.
- 5.2.13.15. Deberá agrupar aplicaciones en categorías existentes y/o personalizadas como: Redes Sociales, P2P, Actualizaciones de Software, Video y Música, entre otros. Así como también se debe poder crear grupos de aplicaciones personalizadas.
- 5.2.13.16. Monitoreo en tiempo real con actualizaciones de como mínimo 5 segundos, que permita realizar un análisis de tráfico en profundidad hasta la búsqueda de una estación de trabajo y un servicio específico, para el diagnóstico de problemas y cuellos de botella en la red.
- 5.2.13.17. La solución debe contar con un dashboard que muestre en tiempo real y en simultáneo distintos gráficos de indicadores del comportamiento y consumo de la red. Mínimamente se requiere tráfico total, aplicaciones de mayor consumo, IP internas o usuarios de mayor consumo, IP externas de mayor consumo y el desempeño de la calidad de las aplicaciones (dependiendo del fabricante este último indicador puede llamarse score de aplicaciones, salud de aplicaciones, entre otros)
- 5.2.13.18. La solución deberá mostrar estadísticas del tráfico de descarga y de subida en un periodo de tiempo configurable
- 5.2.13.19. Deberá permitir la generación reportes basados en gráficos en los cuales se muestre el consumo por IP, subred, aplicaciones, usuarios (requiere integración con el Directorio Activo).
- 5.2.13.20. El equipo deberá permitir el envío de alarmas por medio de email y por traps (snmp)
- 5.2.13.21. El equipo deberá detectar y mostrar anomalías en la red correspondientes a diversos tipos de ataques, enviando alertas y permitiendo la ejecución de acciones automáticas que minimicen su impacto
- 5.2.13.22. Capacidad para detectar usuarios generando exceso de sesiones TCP (DoS, SYN ATTACKS, spoofing) y enviar alertas de eventos.

- 5.2.13.23. El equipo deberá ser capaz de mostrar la geografía del tráfico, es decir contra que países se está realizando el intercambio de datos. Así como soportar la creación de políticas que permitan bloquear el tráfico desde o hacia uno o varios países.
- 5.2.13.24. El equipo deberá poder conectarse con el servidor de actualizaciones del fabricante para que pueda descargar e instalar las actualizaciones remotamente. De esta forma se garantizará que el equipo siempre se encuentre actualizado con la última versión publicada por el fabricante.
- 5.2.13.25. El equipo debe soportar la exportación de información a aplicaciones de colección externa a través de NetFlow, donde el puerto de envío UDP sea configurable
- 5.2.13.26. El equipo debe garantizar el almacenamiento de datos en su disco duro interno de por lo menos los últimos 24 meses, independiente de la presencia de un sistema de colección externa, para la posterior generación de reportes y estadísticas.
- 5.2.13.27. Deberá considerar una consola de administración gráfica en el mismo equipo que permita administrar, configurar y generar reportes del equipo Administrador de Ancho de Banda. Se deberá poder mostrar información de reportes al menos de los últimos 24 meses.
- 5.2.13.28. El software para el manejo de reportes y acceso a la consola de gestión del equipo debe ser provisto en el mismo appliance sin utilizar hardware (servidor) ni software adicional, ni virtualizando el equipo
- 5.2.13.29. Capacidad de limitar el acceso a la consola de gestión web del equipo para un grupo definido de direcciones IP, previniendo el acceso no autorizado al equipo.
- 5.2.13.30. La Entidad deberá contar con acceso de lectura al equipo (4 usuarios) para la obtención de reportes en cualquier momento. Estos usuarios serán distintos a los que tendrá el proveedor del servicio.

#### 6. Modalidad de ejecución contractual

- Llave en mano, siendo responsabilidad del contratista, realizar todo lo referente a los bienes y servicios para su correcta puesta en marcha y funcionamiento.
- Cualquier gasto adicional o imprevisto que incurra motivo del mismo deberá ser asumido por el postor que resulte beneficiado con la buena pro. La entidad no asumirá gastos adicionales por ningún motivo y de ninguna índole.

#### 7. Del Personal clave para la instalación, Implementación y puesta en marcha

##### 7.1. Personal

###### (01) jefe de Proyecto:

- o Actividades:  
Quien tendrá la responsabilidad de la planificación, plan de trabajo y supervisión del desarrollo de la implementación.
- o Perfil:
  - Profesional titulado y/o Grado de Bachiller, como mínimo en una de las siguientes carreras profesionales: Ingeniería Electrónica, Ingeniería de Telecomunicaciones, Ingeniería de Sistemas, Ingeniería de Informática, Ingeniería Industrial, Cómputo.
  - Certificación vigente en Project Management Professional (PMP) o en estudios como especialista en gerencia de proyectos para suscripción de contrato.

###### Un (01) Especialista en Seguridad Perimetral:

- o Actividades:  
Quién tendrá a cargo la instalación, configuración y soporte de los componentes del bien.
- o Perfil:
  - Título o Grado de Bachiller o Título de Técnico como mínimo en una de las siguientes carreras profesionales: Ingeniería de Sistemas y/o Ingeniería Electrónica y/o Ingeniería de Telecomunicaciones y/o carreras profesionales o técnicas afines relacionadas a tecnologías de la información.



Carreras profesionales o técnicas afines: Ingeniería Electrónica y/o Telecomunicación y/o Ingeniería de Computación y/o Ingeniería en Sistemas e Informática y/o Ingeniería Informática y Sistemas y/o Ingeniería de Sistemas de Información y/o Ingeniería de Redes y Comunicaciones y/o Ingeniería Estadística e Informática y/o Administración de Redes y Comunicaciones y/o Administración y Sistemas y/o Redes y Comunicación de Datos y/o Informática y/o Computación y/o Ingeniero de Redes y/o Redes y Comunicaciones de Datos.

- Certificación nivel técnica emitida por el fabricante de la solución ofertada.

○ Para su acreditación, será necesario:

- Copia simple de la Certificación Técnica en la marca o producto ofertado.
- Para acreditar el cumplimiento del perfil del personal, se debe presentar la copia simple del grado de bachiller en ingeniería o copia simple del título técnico, que deberá ser acreditada a la suscripción del contrato.

#### **8. Plazo de entrega**

El plazo de entrega de los equipos y ejecución de los servicios es de 45 días calendario, el plazo será computado a partir del día siguiente de firmado el contrato.

#### **9. Garantía Comercial**

Se deberá proveer una garantía comercial contra defectos de diseño y/o fabricación, averías, por mal funcionamiento o pérdida total de los bienes derivados de desperfectos o fallas ajenas al uso normal o habitual de los bienes, los cuales no fueron detectados en el momento que se otorgó la conformidad, por un periodo de veinticuatro (24) meses.


#### **10. Soporte Técnico**

##### **10.1 Planificación**

- Iniciará a partir del día siguiente de firmado el contrato, y tendrá una duración máxima de 10 días calendario.
- El Postor deberá elaborar y validar el plan de trabajo (Gantt, checklist de pruebas, configuraciones) y arquitectura de la solución con CENARES, para ello será necesario agendar reuniones con el equipo técnico de CENARES.
- El Postor deberá presentar el plan de trabajo (Gantt, checklist de pruebas, configuraciones) y diagrama de arquitectura de la solución.
- Carta del fabricante autorizando al proveedor como representante de la marca en el Perú.
- Diagrama de arquitectura de la solución (formato Visio y Pdf).



#### 10.2 Instalación y Configuración de Firewall

- W
- B
- 10
- ( )
- 
- a. Inicialará al día siguiente de la entrega del equipo firewall en las oficinas de CENARES, la cual deberá realizarse máximo a los 45 días calendario, el plazo será computado a partir del día siguiente de firmado el contrato, y tendrá una duración máxima 21 días calendario. Esta etapa finaliza con la firma del acta de activación del servicio por parte del Postor y CENARES.
  - b. Durante esta etapa el postor realizará la instalación, configuración y pruebas de firewall y sus componentes de la solución:
    - Configuración de políticas de seguridad, incluye la configuración de: IPS, Antivirus y Anti-Spyware o Antimalware, Control de aplicaciones, DoS, Filtro de datos, VPN, Administración de ancho de banda, Configuración de puntos de acceso, etc.
    - Configuración y migración de políticas del firewall antiguo al nuevo y mejoras que proponga el proveedor.
    - Configuración de la consola de administración incluyendo alertas y reportes predefinidos.
  - c. Durante la instalación y configuración del firewall se debe tener en cuenta las siguientes consideraciones:
    - La instalación deberá efectuarse sin afectar las labores de CENARES ni la continuidad de servicios de red.
    - Las actividades de implementación se realizarán en horarios fuera de oficina o en los horarios que se defina con CENARES.
    - EL postor deberá proveer, instalar, realizar pruebas y configurar óptimamente todo lo solicitado para la puesta en producción del firewall, en coordinación con CENARES.
    - Para la instalación y configuración el postor deberá tener personal especializado, capacitado y/o certificado en el producto ofertado.
  - d. Carta de garantía emitida por el fabricante por dos (02) años (incluir números de serie o número de parte o identificador de cliente).
  - e. Carta de Garantía y Soporte emitida por el Postor por dos (02) años (incluir números de serie).
  - f. Matriz de escalamiento del servicio.
  - g. Procedimiento (flujograma) para la atención de incidentes.
  - h. Informe y acta de instalación y configuración del firewall (acta de activación del servicio).
  - i. La solución deberá ser implementado en el centro de datos de la entidad.
  - j. Los equipos de seguridad perimetral deben ser instalados y configurados uno de protección a los accesos del internet y otro para la protección de la red de datos del centro nacional de abastecimiento de recursos estratégicos de salud - CENARES. Para lo cual se debe incluir todo lo necesario para su óptimo funcionamiento. (Actualización de firmware del equipo, Instalación de equipo en el gabinete, Conexión del equipo a la red eléctrica, Conexión y etiquetado de cables, Configuración de los equipos de seguridad perimetral y el software de administración).
  - k. Todo el material utilizado en la instalación (cables, conectores, adaptadores, etc.) deberá ser suministrado por el proveedor y deberá ir alineadas con las características

de los equipos:

1. En caso de cambio de sede o lugar de instalación inicial dentro del periodo de contrato, el proveedor asumirá a todo costo el traslado del servicio, este cambio se dará solamente en Lima metropolitana.

### **11. Capacitación**

Capacitación certificada por la marca del producto para dos (02) personas del Equipo de Informática del CENARES, en configuración, operación, solución de problemas y mejoras de uso de los equipos de la Solución Ofertada según lo siguiente:

Para los equipos de Seguridad Perimetral.

- Tipo de Capacitación: Deberá seguir el modelo curricular del curso Oficial o currículo similar a la indicada por el fabricante.
- Número de Horas: 16 Horas lectivas

La capacitación se realizará en la Sede Central sito en la Jr. Nazca 548 - Lima 11 - Perú y/o virtual según la coyuntura actual, durante la fase de implementación.

1. Las capacitaciones se realizarán máximo dentro de los cinco (05) días calendario siguientes de la configuración y activación de la licencia, previa coordinación con el área informática de CENARES.
2. El postor deberá incluir la certificación oficial para cada uno de los participantes.

#### **Curso de Cybersecurity:**

Se deberá brindar curso de Cybersecurity para dos (02) profesionales del Equipo de Informática del CENARES, considerando los siguientes objetivos finales:

#### **Generalidades:**

##### **Análisis forense digital en Windows**

A través de un incidente de ataque cibernético simulado en la vida real, el curso deberá cubrir los siguientes temas:

- Introducción a la ciencia forense digital
- Respuesta en vivo y adquisición de evidencia
- Análisis post-mortem de máquinas Windows
- Elementos internos del registro del sistema operativo Windows
- Eventos del sistema operativo Windows
- Análisis de artefactos del sistema operativo Windows
- Exploradores de artefactos forenses
- Análisis de correo electrónico
- Desafíos forenses con discos SSD
- Recomendaciones al construir un laboratorio forense digital



- Probar las habilidades recién adquiridas con un desafío práctico utilizando diferentes artefactos de Windows

#### **Análisis de malware e ingeniería inversa**

- Análisis básico con IDA Pro
- Análisis dinámico utilizando depuradores y soluciones de virtualización populares
- Análisis de documentos maliciosos
- Desembalaje
- Descifrado
- Análisis de Shellcodes
- Análisis de exploits
- Consejos y trucos para revertir

#### **Análisis forense digital avanzado de Windows**

A través de un incidente de ataque cibernético simulado en la vida real, el curso cubrirá los siguientes temas:

- Sistemas numéricos
- Sistema de archivos FAT
- Sistema de archivos NTFS
- Análisis forense profundo de Windows
- Recuperación de datos y archivos del sistema de archivos, instantáneas y uso de la talla de archivos
- Desafíos forenses en la computación en la nube
- Análisis forense de la memoria
- Análisis forense de redes
- Análisis de línea de tiempo frente a SuperTimeline
- Probar las habilidades recién adquiridas con un desafío práctico con evidencia digital adquirida

#### **Análisis avanzado de malware e ingeniería inversa**

- Desembalaje
- Descifrado
- Desarrollo de descifradores propios para escenarios comunes.
- Descompilación de códigos de bytes
- Descomposición de código
- Desmontaje
- Reconstrucción de arquitecturas APT modernas
- Reconocer construcciones de código típicas
- Identificación de algoritmos criptográficos y de compresión
- Clasificación y atribución basada en código y datos
- Reconstrucción de clases y estructuras





- Arquitecturas de complementos APT (basadas en muestras APT recientes)

#### **Respuesta ante incidentes de Windows**

En un entorno simulado de la vida real, se producirá un incidente y el curso cubrirá los siguientes temas en ese escenario:

- Presentación del proceso de respuesta a incidentes y su flujo de trabajo.
- Explicar la diferencia entre amenazas normales y APT.
- Explicación de APT Cyber Kill Chain
- Aplicar el proceso de respuesta a incidentes a diferentes escenarios de incidentes
- Aplicar Cyber Kill Chain en el entorno simulado
- Aplicación de análisis en vivo en máquinas de víctimas para los socorristas
- Técnicas de adquisición de pruebas sólidas desde el punto de vista forense
- Introducción al análisis post mortem y la ciencia forense digital
- Introducción al análisis forense de la memoria
- Análisis de archivos de registro con expresiones regulares y ELK
- Introducción de inteligencia sobre amenazas cibernéticas
- Creación de IoC (indicadores de compromiso), con YARA y SNORT
- Introducción al análisis de malware y la zona de pruebas
- Introducción al análisis forense del tráfico de red
- Discutir informes de análisis de incidentes y recomendaciones sobre la creación de CSIRT
- Probar las habilidades recién adquiridas con un desafío práctico en otro escenario simulado

#### **Detección eficiente de amenazas con Yara**

- Breve introducción a la sintaxis de Yara
- Consejos y trucos para crear reglas rápidas y efectivas
- Generadores Yara
- Prueba de las reglas de Yara para detectar falsos positivos
- Búsqueda de nuevas muestras no detectadas en VT
- Uso de módulos externos dentro de Yara para una caza eficaz
- Búsqueda de anomalías
- Muchos Ejemplos de la vida real
- Un conjunto de ejercicios para mejorar las habilidades en Yara



#### **12. Lugar de entrega**

Los bienes deberán ser entregados en, sito en Av. Independencia N.º 1837 - El Agustino.  
Horario de oficina (10:00 a.m. a 1:00p.m. o 2:00 p.m. a 4:00 p.m.).

### **13. Conformidad**

La conformidad será proporcionada por el Equipo de Informática del Centro de Gestión Administrativa luego de haber realizado la verificación de las características técnicas del equipo adquirido y su implementación en el centro de datos del CENARES.

### **14. 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.

### **15. Otras condiciones**

- Las especificaciones técnicas deben considerarse como mínimas indispensables, pudiendo el proveedor proponer un equipo superior, sin costo adicional para la Entidad. Se considerará superior siempre y cuando supere todas las características técnicas solicitadas.
- El CENARES se reserva el derecho de comprobar la veracidad de toda la información proporcionada por el postor.
- La recepción de conformidad no invalida el reclamo posterior por parte de la Entidad, por defectos e inadecuación a las especificaciones técnicas u otras situaciones anómalas no detectables o no verificables durante la recepción de los equipos.
- El proveedor deberá dejar en completo funcionamiento el equipo, para lo cual deberá considerar los cables y accesorios necesarios para conectar los equipos y certificar su correcto funcionamiento.
- El proveedor deberá de tomar todas las previsiones del caso con la finalidad de que la solución que oferte se implemente sin inconvenientes, garantizando en todo momento la continuidad operativa de los servicios informáticos de la entidad que puedan verse afectado por la implementación de la solución.
- Transferencia de conocimiento de la solución instalada.

### **16. Confidencialidad**

El contratista está obligado a guardar la confidencialidad y reserva absoluta en el manejo de información y documentación a la que tenga acceso y que se encuentra relacionada con la prestación, quedando expresamente prohibido revelar dicha información.



### **17. 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 de su reglamento, 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.

### **18. Penalidad**

Si el contratista incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, la Entidad le aplicará una penalidad por cada día de atraso, hasta por un monto máximo equivalente al diez por ciento (10%) del monto del contrato vigente, en concordancia con el artículo 162 del Reglamento de la Ley de Contrataciones del Estado. En todos los casos,

la penalidad se aplicará automáticamente y se calculará de acuerdo a la siguiente fórmula:

En todos los casos, la penalidad se aplicará automáticamente y se calculará de acuerdo a la siguiente fórmula:

$$\text{Penalidad Diaria} = \frac{0,10 \times \text{Monto}}{F \times \text{Plazo en días}}$$

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

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

a.1) Para bienes, servicios en general y consultorías:  $F = 0.25$

#### **19. 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:

- I. Alcohol en gel o soluciones desinfectantes
- II. 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.

20. Requisitos de calificación

B.	<b>EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD</b>
	<p><b><u>Requisitos:</u></b> El postor debe acreditar un monto facturado acumulado equivalente a S/ 480,000.00 (Cuatrocientos Ochenta Mil con 00/100 soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran bienes similares a los siguientes: Equipos de seguridad perimetral Firewall y/o equipos de seguridad informática y/o equipos de comunicaciones para centro de datos y/o Equipos de IPS.</p> <p><b><u>Acreditación:</u></b> 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 vóucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago<sup>1</sup> correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 7 referido a la Experiencia del Postor en la Especialidad.</p>



<sup>1</sup> Cabe precisar que, de acuerdo con la Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado:

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

(...)

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

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

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

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

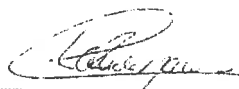
Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de una persona absorbida 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.

C.	CAPACIDAD TECNICA Y PROFESIONAL
C.1	EXPERIENCIA DEL PERSONAL CLAVE
	<p>El postor deberá contar con el siguiente personal especialista encargado de la ejecución del proyecto, conforme a lo siguiente:</p> <p><b>Requisito:</b></p> <p><b>(01) jefe de Proyecto:</b></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><b>Acreditación:</b></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><b>(01) Especialista en Seguridad Perimetral.</b></p> <ul style="list-style-type: none"><li>▪ Dos (02) años realizando funciones en: Solución de Seguridad Perimetral y/o Configuración de seguridad perimetral, y/o diseño de seguridad perimetral y/o Configuración de IPS y/o Configuración de IDS.</li></ul> <p><b>Acreditación:</b></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>

  
ING. CARCLA RAMIREZ DIOS DE CACHO  
Responsable de Equipos de Informática  
CENARES - MINSA

### Importante

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

## 3.2. REQUISITOS DE CALIFICACIÓN

B	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><b>Requisitos:</b></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/ 480,000.00 (Cuatrocientos Ochenta Mil con 00/100 soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>Se consideran bienes similares a los siguientes Equipos de seguridad perimetral Firewall y/o equipos de seguridad informática y/o equipos de comunicaciones para centro de datos y/o equipos de IPS.</p> <p><b>Acreditación:</b></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 pago<sup>6</sup>, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el 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 obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.</p> <p>Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.</p> <p>Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.</p>

<sup>6</sup> Cabe precisar que, de acuerdo con la Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado:

"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehacencia 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".

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".*

<b>C</b>	<b>CAPACIDAD TÉCNICA Y PROFESIONAL</b>
<b>C.1</b>	<b>EXPERIENCIA DEL PERSONAL CLAVE</b>
	<p><u>Requisitos:</u></p> <ul style="list-style-type: none"> <li>- <b>Un (1) Jefe de Proyecto</b> Requisitos Dos (2) años realizando actividades en: gestión de proyectos de tecnologías de la información y/o seguridad perimetral, y/o seguridad de información, y/ plan director de seguridad.</li> <li>- <b>Un (1) Especialista en Seguridad Perimetral</b> Requisitos Dos (2) años realizando funciones en: solución de Seguridad Perimetral y/o configuración de seguridad perimetral, y/o diseño de seguridad perimetral y/o configuración de IPS y/o configuración de IDS.</li> </ul> <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><b>Importante</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.</li> <li>• 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.</li> <li>• Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.</li> </ul>

**Importante**



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

B  
W  
Q



**CAPÍTULO IV  
FACTORES DE EVALUACIÓN**

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

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

FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
<b>A. PRECIO</b>	
<p><u>Evaluación:</u></p> <p>Se evaluará considerando el precio ofertado por el postor.</p> <p><u>Acreditación:</u></p> <p>Se acreditará mediante el registro en el SEACE o el documento que contiene el precio de la oferta (<b>Anexo N° 6</b>), 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> $PI = \frac{Om \times PMP}{OI}$ <p>I = Oferta PI = Puntaje de la oferta a evaluar OI = Precio I Om = Precio de la oferta más baja PMP = Puntaje máximo del precio</p> <p style="text-align: right;"><b>100 puntos</b></p>

**Importante**

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

## CAPÍTULO V PROFORMA DEL CONTRATO

### Importante

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

Conste por el presente documento, la contratación de Adquisición de Equipo de Seguridad Perimetral - Firewall, que celebra de una parte [CONSIGNAR EL NOMBRE DE LA ENTIDAD], 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 adjudicó la buena pro de la LICITACIÓN PÚBLICA N° 008-2021-CENARES/MINSA para la contratación de [CONSIGNAR LA DENOMINACIÓN DE LA CONVOCATORIA], a [INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO], cuyos detalles e importe constan en los documentos integrantes del presente contrato.

### CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto la Adquisición de Equipo de Seguridad Perimetral - Firewall.

N° Ítem	Descripción del Bien
1	01 NGFW de protección perimetral de acceso al internet CENARES
	01 NGFW de protección al centro de datos CENARES

### CLÁUSULA TERCERA: MONTO CONTRACTUAL

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

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

### CLÁUSULA CUARTA: DEL PAGO<sup>7</sup>

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

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.

<sup>7</sup> En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.

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, LUGAR DE LA EJECUCIÓN DE LA PRESTACIÓN**

El plazo de ejecución del presente contrato es de cuarenta y cinco (45) días calendario, el mismo que se computa desde el día siguiente de suscrito el contrato.

**Planificación**

- Iniciaré a partir del día siguiente de firmado el contrato, y tendrá una duración máxima de 10 días calendario.
- El Postor deberá elaborar y validar el plan de trabajo (Gantt, checklist de pruebas, configuraciones) y arquitectura de la solución con CENARES, para ello será necesario agendar reuniones con el equipo técnico de CENARES.
- El Postor deberá presentar el plan de trabajo (Gantt, checklist de pruebas, configuraciones) y diagrama de arquitectura de la solución.
- Carta del fabricante autorizando al proveedor como representante de la marca en el Perú.
- Diagrama de arquitectura de la solución (formato Visio y Pdf).

**Instalación y Configuración de Firewall**

- a. Iniciaré al día siguiente de la entrega del equipo firewall en las oficinas de CENARES, la cual deberá realizarse máximo a los 45 días calendario, el plazo será computado a partir del día siguiente de firmado el contrato, y tendrá una duración máxima 21 días calendario. Esta etapa finaliza con la firma del acta de activación del servicio por parte del Postor y CENARES.
- b. Durante esta etapa el postor realizará la instalación, configuración y pruebas de firewall y sus componentes de la solución:
  - Configuración de políticas de seguridad, incluye la configuración de: IPS, Antivirus y Anti-Spyware o Antimalware, Control de aplicaciones, DoS, Filtro de datos, VPN, Administración de ancho de banda, Configuración de puntos de acceso, etc.
  - Configuración y migración de políticas del firewall antiguo al nuevo y mejoras que proponga el proveedor.
  - Configuración de la consola de administración incluyendo alertas y reportes predefinidos.
- c. Durante la instalación y configuración del firewall se debe tener en cuenta las siguientes consideraciones:
  - La instalación deberá efectuarse sin afectar las labores de CENARES ni la continuidad de servicios de red.
  - Las actividades de implementación se realizarán en horarios fuera de oficina o en los horarios que se defina con CENARES.
  - El postor deberá proveer, instalar, realizar pruebas y configurar óptimamente todo lo solicitado para la puesta en producción del firewall, en coordinación con CENARES.
  - Para la instalación y configuración el postor deberá tener personal especializado, capacitado y/o certificado en el producto ofertado.
- d. Carta de garantía emitida por el fabricante por dos (02) años (incluir números de serie o número de parte o identificador de cliente).
- e. Carta de Garantía y Soporte emitida por el Postor por dos (02) años (incluir números de serie).
- f. Matriz de escalamiento del servicio.
- g. Procedimiento (flujograma) para la atención de incidentes.
- h. Informe y acta de instalación y configuración del firewall (acta de activación del servicio).
- i. La solución deberá ser implementado en el centro de datos de la entidad.
- j. Los equipos de seguridad perimetral deben ser instalados y configurados uno de protección a los accesos del internet y otro para la protección de la red de datos del centro nacional de abastecimiento de recursos estratégicos de salud - CENARES. Para lo cual se debe incluir todo lo necesario para su óptimo funcionamiento. (Actualización de firmware del equipo, Instalación de equipo en el gabinete, Conexión del equipo a la red eléctrica,

Conexión y etiquetado de cables, Configuración de los equipos de seguridad perimetral y el software de administración).

- k. Todo el material utilizado en la instalación (cables, conectores, adaptadores, etc.) deberá ser suministrado por el proveedor y deberá ir alineadas con las características de los equipos.
- l. En caso de cambio de sede o lugar de instalación inicial dentro del periodo de contrato, el proveedor asumirá a todo costo el traslado del servicio, este cambio se dará solamente en lima metropolitana.

#### **LUGAR DE ENTREGA**

Los bienes deberán ser entregados en sito en Av. Independencia N° 1837 - El Agustino. Horario de oficina (10:00 a.m. a 1:00p.m. o 2:00 p.m. a 4:00 p.m.).

#### **CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO**

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

#### **CLÁUSULA SÉTIMA: GARANTÍAS**

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

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

En el caso que corresponda, consignar lo siguiente:

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

#### **Importante**

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

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

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

#### **CLÁUSULA NOVENA: RECEPCIÓN Y CONFORMIDAD DE LA PRESTACIÓN**

La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La recepción será otorgada por el responsable del Almacén y la conformidad será otorgada por el Equipo de Informática del Centro de Gestión Administrativa en el plazo máximo de siete (7) días de producida la recepción.

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

Handwritten marks: a stylized 'P' and 'W' followed by a circle containing the number '10'.

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 DÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA**

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

**CLÁUSULA UNDÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS**

La 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) años contado a partir de la conformidad otorgada por LA ENTIDAD.

**CLÁUSULA DUODÉCIMA: PENALIDADES**

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

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

Donde:

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

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

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

**Importante**

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

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

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

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

**CLÁUSULA DÉCIMA TERCERA: RESOLUCIÓN DEL CONTRATO**

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

**CLÁUSULA DÉCIMA CUARTA: RESPONSABILIDAD DE LAS PARTES**

Cuando se resuelva el contrato por causas imputables a algunas de las partes, se debe resarcir los

daños y perjuicios ocasionados, a través de la indemnización correspondiente. Ello no obsta la aplicación de las sanciones administrativas, penales y pecuniarias a que dicho incumplimiento diere lugar, en el caso que éstas correspondan.

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

**CLÁUSULA DÉCIMA QUINTA: ANTICORRUPCIÓN**

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

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

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

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

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

**CLÁUSULA DÉCIMA SÉTIMA: SOLUCIÓN DE CONTROVERSIAS<sup>8</sup>**

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

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

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

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

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

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

**CLÁUSULA DÉCIMA NOVENA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL**

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

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

<sup>8</sup> De acuerdo con el numeral 225.3 del artículo 225 del Reglamento, las partes pueden recurrir al arbitraje ad hoc cuando las controversias deriven de procedimientos de selección cuyo valor estimado sea menor o igual a cinco millones con 00/100 soles (S/ 5 000 000,00).

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

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

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

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

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

Handwritten signature and initials on the left margin.



## **ANEXOS**

F  
W  
D

**ANEXO N° 1**

**DECLARACIÓN JURADA DE DATOS DEL POSTOR**

Señores  
**COMITÉ DE SELECCIÓN**  
**LICITACIÓN PÚBLICA N° 008-2021-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) :		
Correo electrónico :			

**Autorización de notificación por correo electrónico:**

... [CONSIGNAR SÍ O NO] autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.
4. Respuesta a la solicitud de acceso al expediente de contratación.
5. Notificación de la orden de compra<sup>9</sup>

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

[CONSIGNAR CIUDAD Y FECHA]

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

**Importante**

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

<sup>9</sup> Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de compra.

**Importante**

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

**ANEXO N° 1**

**DECLARACIÓN JURADA DE DATOS DEL POSTOR**

Señores  
**COMITÉ DE SELECCIÓN**  
**LICITACIÓN PÚBLICA N° 008-2021-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:

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

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

<b>Datos del consorciado ...</b>			
Nombre, Denominación o Razón Social :			
Domicilio Legal :			
RUC :		Teléfono(s) :	
Correo electrónico :			

**Autorización de notificación por correo electrónico:**

Correo electrónico del consorcio:

... [CONSIGNAR SÍ O NO] autorizo que se notifiquen al correo electrónico indicado las siguientes actuaciones:

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.
4. Respuesta a la solicitud de acceso al expediente de contratación.
5. Notificación de la orden de compra<sup>10</sup>

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

[CONSIGNAR CIUDAD Y FECHA]

<sup>10</sup> Consignar en el caso de procedimientos de selección por relación de ítems, cuando el monto del valor estimado del ítem no supere los doscientos mil Soles (S/ 200 000.00), cuando se haya optado por perfeccionar el contrato con una orden de compra.

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

**Importante**

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

R  
W  
D

**ANEXO N° 2**

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

Señores  
**COMITÉ DE SELECCIÓN**  
**LICITACIÓN PÚBLICA N° 008-2021-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**  
**LICITACIÓN PÚBLICA N° 008-2021-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]

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

**Importante**

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

**ANEXO N° 4**

**DECLARACIÓN JURADA DE PLAZO DE ENTREGA**

Señores  
**COMITÉ DE SELECCIÓN**  
**LICITACIÓN PÚBLICA N° 008-2021-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**  
**LICITACIÓN PÚBLICA N° 008-2021-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 **LICITACIÓN PÚBLICA N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]**.

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

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

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

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

1. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] [ % ]<sup>11</sup>

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [ % ]<sup>12</sup>

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES

100%<sup>13</sup>

[CONSIGNAR CIUDAD Y FECHA]

<sup>11</sup> Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

<sup>12</sup> Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

<sup>13</sup> Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.



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

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

**Importante**

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

3  
W  
0

**ANEXO N° 6**

**PRECIO DE LA OFERTA**

Señores  
**COMITÉ DE SELECCIÓN**  
**LICITACIÓN PÚBLICA N° 008-2021-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
<b>TOTAL</b>	

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]"*.

ANEXO N° 7

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores  
**COMITÉ DE SELECCIÓN**  
**LICITACIÓN PÚBLICA N° 008-2021-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 <sup>14</sup>	FECHA DE LA CONFORMIDAD DE SER EL CASO <sup>15</sup>	EXPERIENCIA PROVENIENTE <sup>16</sup> DE:	MONEDA	IMPORTE <sup>17</sup>	TIPO DE CAMBIO VENTA <sup>18</sup>	MONTO FACTURADO ACUMULADO <sup>19</sup>
1										
2										
3										
4										

<sup>14</sup> Se refiere a la fecha de suscripción del contrato, de la emisión de la Orden de Compra o de cancelación del comprobante de pago, según corresponda.

<sup>15</sup> Únicamente, cuando la fecha del perfeccionamiento del contrato, sea previa a los ocho (8) años anteriores a la fecha de presentación de ofertas, caso en el cual el postor debe acreditar que la conformidad se emitió dentro de dicho periodo.

<sup>16</sup> Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Al respecto, según la Opinión N° 216-2017/DTN "Considerando que la sociedad matriz y la sucursal constituyen la misma persona jurídica, la sucursal puede acreditar como suya la experiencia de su matriz". Del mismo modo, según lo previsto en la Opinión N° 010-2013/DTN, "... en una operación de reorganización societaria que comprende tanto una fusión como una escisión, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad incorporada o absorbida, que se extingue producto de la fusión; asimismo, si en virtud de la escisión se transfiere un bloque patrimonial consistente en una línea de negocio completa, la sociedad resultante podrá acreditar como suya la experiencia de la sociedad escindida, correspondiente a la línea de negocio transmitida. De esta manera, la sociedad resultante podrá emplear la experiencia transmitida, como consecuencia de la reorganización societaria antes descrita, en los futuros procesos de selección en los que participe".

<sup>17</sup> Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

<sup>18</sup> El tipo de cambio venta debe corresponder al publicado por la SBS correspondiente a la fecha de suscripción del contrato, de la emisión de la Orden de Compra o de cancelación del comprobante de pago, según corresponda.

<sup>19</sup> Consignar en la moneda establecida en las bases.

CENTRO NACIONAL DE ABASTECIMIENTO DE RECURSOS ESTRATÉGICOS EN SALUD - CENARES  
LICITACIÓN PÚBLICA N° 008-2021-CENARES/MINSA

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/C / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP <sup>14</sup>	FECHA DE LA CONFORMIDAD DE SER EL CASO <sup>15</sup>	EXPERIENCIA PROVENIENTE <sup>16</sup> DE:	MONEDA	IMPORTE <sup>17</sup>	TIPO DE CAMBIO VENTA <sup>18</sup>	MONTO FACTURADO ACUMULADO <sup>19</sup>
5										
6										
7										
8										
9										
10										
...										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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



**ANEXO N° 8**

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

Señores  
**COMITÉ DE SELECCIÓN**  
**LICITACIÓN PÚBLICA N° 008-2021-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.*