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

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

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

SIMBOLOGÍA UTILIZADA:

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

CARACTERÍSTICAS DEL DOCUMENTO:

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

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

INSTRUCCIONES DE USO:

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

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

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

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

CONCURSO PÚBLICO Nº *005-2024-FAP/SINFA*

CONTRATACIÓN DE SERVICIO DE RENOVACIÓN DE LICENCIAS, EXTENSIÓN DE SOPORTE Y GARANTÍA DE LOS EQUIPOS DE TECNOLOGÍA DE LA INFORMACIÓN DEL CENTRO DE DATOS SINFA

DEBER DE COLABORACIÓN

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

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

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

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

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I
ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

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

Importante

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

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

Importante

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

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

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

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

Advertencia

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

Importante

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

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

Las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita o digital, según la Ley Nº 27269, Ley de Firmas y Certificados Digitales[1]). Los demás documentos deben ser visados

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

por el postor. En el caso de persona jurídica, por su representante legal, apoderado o mandatario designado para dicho fin y, en el caso de persona natural, por este o su apoderado. No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas.

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

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

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

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

1.9. EVALUACIÓN DE LAS OFERTAS

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

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

1.10. CALIFICACIÓN DE OFERTAS

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

1.11. SUBSANACIÓN DE LAS OFERTAS

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

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

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

1.12. RECHAZO DE LAS OFERTAS

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

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

1.13. OTORGAMIENTO DE LA BUENA PRO

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

1.14. CONSENTIMIENTO DE LA BUENA PRO

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

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

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

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

CAPÍTULO II
SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

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

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

Importante

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

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

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

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

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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

CAPÍTULO III
DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

En las contrataciones que conllevan la ejecución de prestaciones accesorias, tales como mantenimiento, reparación o actividades afines, se otorga una garantía adicional por una suma equivalente al diez por ciento (10%) del monto del contrato de la prestación 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.*

- *En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establecen los numerales 149.4 y 149.5 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento.*

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

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

Importante

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

Advertencia

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

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

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

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

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

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

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

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

3.4. EJECUCIÓN DE GARANTÍAS

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

3.5. ADELANTOS

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

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

3.6.2. OTRAS PENALIDADES

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

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

3.7. INCUMPLIMIENTO DEL CONTRATO

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

3.8. PAGOS

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

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

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

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

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

3.9. DISPOSICIONES FINALES

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

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I
GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre	:	FUERZA AÉREA DEL PERÚ
RUC Nº	:	20144364059
Domicilio legal	:	Av. de la Peruanidad S/N – Jesús María
Teléfono:	:	973956725
Correo electrónico:	:	Adquisiciones.secre2024@gmail.com

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del servicio de **SERVICIO DE RENOVACIÓN DE LICENCIAS, EXTENSIÓN DE SOPORTE Y GARANTÍA DE LOS EQUIPOS DE TECNOLOGÍA DE LA INFORMACIÓN DEL CENTRO DE DATOS SINFA**

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Resolución Directoral N° 00175 /DIGLO del 24 de abril de 2024.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios

1.5. SISTEMA DE CONTRATACIÓN

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

1.6. DISTRIBUCIÓN DE LA BUENA PRO

No corresponde para el presente proceso.

1.7. ALCANCES DEL REQUERIMIENTO

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

1.8. PLAZO DE PRESTACIÓN DEL SERVICIO

Los servicios materia de la presente convocatoria se prestarán en el plazo de sesenta y cinco (65) días calendarios, contabilizados desde el día establecido en el contrato, en concordancia con lo establecido en el expediente de contratación. El plazo de duración del servicio será, de acuerdo al cuadro adjunto:

Actividades	Plazo
Se realizarán siete (7) actividades previas a la presentación del informe final por parte del postor	**El plazo para la realización de las siete (7) actividades será de sesenta (65) días calendarios de acuerdo con el siguiente detalle:**
Actividad N° 1: Extensión de Suscripción de Licencias para 500 Buzones del Antispam Cisco ESA C195 y soporte de fábrica de hardware y software.	Del 9 hasta el 21 de julio del 2024 para la ejecución de la actividad y la transferencia de conocimientos de ocho (8) horas para la presente solución.
Actividad N° 2: Extensión de soporte fábrica de Hardware y Software de la solución de respaldo y restauración Veritas Netbackup 5240	Del 22 de julio hasta el 1 de agosto del 2024 para la ejecución de la actividad y la transferencia de conocimientos de ocho (8) horas para la presente solución.
Actividad N° 3: Extensión de Suscripción de Licencias, soporte de fábrica de hardware y software del Firewall CheckPoint 5600 **Actividad N° 4:** Extensión de Suscripción de Licencias, soporte de fábrica de hardware y software del Firewall CheckPoint 5900. **Actividad N° 5**: Extensión de Suscripción de Licencias, soporte de fábrica de hardware y software del CheckPoint Sandblast. TE-1000X	Del 2 hasta el 16 de agosto del 2024 para la ejecución de la actividad y la transferencia de conocimientos de ocho (8) horas para las presentes soluciones.
Actividad N° 6: Extensión de soporte y garantía de fábrica Hardware y Software del DNS, DHCP, IPAM Infoblox Trinzic 1405	Del 17 hasta el 26 de agosto del 2024 para la ejecución de la actividad y la transferencia de conocimientos de ocho (8) horas para la presente solución.
Actividad N° 7: Extensión de soporte y garantía de fabrica Hardware y Software del balanceador de carga/SSL A10 Thunder 3030s, y presentación del informe final	Del 27 de agosto hasta el 11 de setiembre del 2024 para la ejecución de la actividad y la transferencia de conocimientos de ocho (8) horas para la presente solución, y presentación del informe final

1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases, para cuyo efecto deben cancelar el costo de las fotocopias.

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

1.10. BASE LEGAL

- Ley Nº 43610 Ley de Presupuesto del Sector Público para el Año Fiscal 2024
- Ley Nº 31954 Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2024.
- Ley N° 30225, Ley de Contrataciones del Estado, en adelante la Ley y sus modificatorias.
- Decreto Supremo N° 344-2018-EF, Reglamento de la Ley de Contrataciones del Estado, en adelante el Reglamento y sus modificatorias.
- Ley Nº 27444, Ley del Procedimiento Administrativo General.

- Ley Nº 27806, Ley de Transparencia y de Acceso a la Información Pública.
- Código Civil.

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

CAPÍTULO II
DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

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

2.2. CONTENIDO DE LAS OFERTAS

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

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

a) Declaración jurada de datos del postor. (**Anexo Nº 1)**

b) Documento que acredite la representación de quien suscribe la oferta.

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

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

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

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

c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento. **(Anexo Nº 2)**

d) Declaración jurada de cumplimiento de los Términos de Referencia

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

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

contenidos en el numeral 3.1 del Capítulo III de la presente sección. (**Anexo Nº 3**)

e) Documento que indique el tipo de licencias propuestas para renovación con sus respectivas listas de funcionalidades y/o Blades, que cumplan lo solicitado en los términos de referencia.
f) Carta del fabricante indicando ser partner autorizado del postor, de cada una de las licencias propuestas indicada carta deberá hacer referencia a presente Concurso Público.

g) Declaración jurada de plazo de prestación del servicio. **(Anexo Nº 4)**[4]

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 Nº 5**)

i) El precio de la oferta en soles. Adjuntar obligatoriamente el **Anexo Nº 6.**

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

Importante

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

2.2.1.2. Documentos para acreditar los requisitos de calificación

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

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

a) Garantía de fiel cumplimiento del contrato.
b) Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso.
c) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes de ser el caso.
d) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y la entidad bancaria en el exterior.
e) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
f) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de

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

persona jurídica.

Advertencia

*De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las Entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE**5** y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f).*

g) Domicilio para efectos de la notificación durante la ejecución del contrato.
h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación 6 (**Anexo N° 12**).
i) Detalle de los precios unitarios del precio ofertado[7].
j) Estructura de costos[8].
k) Detalle del precio de la oferta de cada uno de los servicios que conforman el paquete[9].
l) Plan de Trabajo con su respectivo cronograma en función a los horarios laborales (7:45 a 16:45 horas de lunes a viernes)

Importante

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

- *En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por la Entidad durante la primera mitad del número total de pagos a realizarse, de forma prorrateada en cada pago, con cargo a ser devuelto a la finalización del mismo, conforme lo establece el numeral 149.4 del artículo 149 del Reglamento y numeral 151.2 del artículo 151 del Reglamento. Para dicho efecto los postores deben encontrarse registrados en el REMYPE, consignando en la Declaración Jurada de Datos del Postor (Anexo N° 1) o en la solicitud de retención de la garantía durante el perfeccionamiento del contrato, que tienen la condición de MYPE, lo cual será verificado por la Entidad en el link http://www2.trabajo.gob.pe/servicios-en-linea-2-2 opción consulta de empresas acreditadas en el REMYPE.*

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

Importante

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

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

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

8 Incluir solo cuando resulte necesario para la ejecución contractual, identificar los costos de cada uno de los rubros que comprenden la oferta.

9 Incluir solo en caso de contrataciones por paquete.

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

- *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya[10].*

- *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 la oficina de Abastecimiento del Servicio de Informática, ubicado en el Block B del Cuartel General de la FAP, Av. La Peruanidad S/N Jesús María.

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en PAGO ÚNICO, posterior a la conformidad del servicio.

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

- Informe del funcionario responsable del Departamento de Arquitectura Digital, emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.
- Informe Técnico especializado del representante de la empresa contratista (con fotografías del antes, durante y después), incluyendo el acta de transferencia de conocimientos.

Dicha documentación se debe presentar en oficina de Abastecimiento del Servicio de Informática, ubicado en el Block B del Cuartel General de la FAP, Av. La Peruanidad S/N Jesús María

10 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. TERMINOS DE REFERENCIA

1.- DENOMINACIÓN DEL SERVICIO

"Servicio de Renovación de Licencias y Extensión de Soporte y Garantía de los Equipos de Tecnología de Información del Centro de Datos FAP"

2.- FINALIDAD PÚBLICA

Renovar y extender el licenciamiento y suscripción, soporte y garantías de los equipos de Tecnologías de Información en el Centro de Datos Institucional (CDI) lo cual permitirá mantener la funcionalidad de los diversos sistemas y aplicaciones albergados en el CDI.

3.- OBJETO DEL SERVICIO

Realizar la instalación de llaves de licenciamiento y suscripciones además de extender el soporte y garantías del equipamiento de seguridad, conectividad y respaldo ubicados en el CDI, a fin de asegurar el óptimo funcionamiento de los componentes y de esta manera garantizar la disponibilidad integridad y confidencialidad de los servicios, sistemas y aplicaciones FAP, administrados por este SINFA.

4.- ALCANCE Y DESCRIPCIÓN DEL SERVICIO A CONTRATAR

En el presente servicio se realizará la extensión de las licencias y/o suscripciones y la entrega de la constancia por parte de la marca de la renovación de soporte y garantía de los equipos. El postor deberá realizar pruebas de funcionamiento a fin de validar que la solución no afecte la disponibilidad de ninguno de los servicios, sistema o aplicación de uso institucional dejando operativo los servicios de TI involucrados en este proceso.

El servicio consta de las siguientes soluciones:

a.- **Extensión de Suscripción de Licencias para 500 Buzones del Antispam Cisco ESA C195 y soporte de fábrica de hardware y software.**

La extensión de la suscripción para los 500 buzones del Cisco ESA C195 debe considerar:

1) Antispam
2) Antimalware
3) Detección de graymail
4) Solución de antivirus
5) Outbreak filters
6) Detección de correo electrónico falsificado
7) Filtro de contenido

Estas características se deben considerar para correos entrantes y salientes, además el postor deberá garantizar el soporte de software pudiendo elevar el caso a la marca si fuese necesario.

Se tendrá que hacer una revisión y hardening de las políticas implementadas. Asimismo, se tendrá soporte de la marca para casos de fallo de hardware incluyendo la autorización de retorno de mercadería (RMA).

Como parte de los entregables el proveedor deberá remitir el certificado expedido por la marca por la renovación de suscripción de licencia del 12-07-2024 hasta el 31-12-2025.

b.- **Extensión de soporte fábrica de hardware y software de la solución de respaldo y restauración Veritas Netbackup 5240**

La extensión de soporte y garantía de la solución debe contemplar las siguientes funcionalidades del equipo:

1) Protección
a) Integridad de datos con inmutabilidad independiente del almacenamiento.
b) Control de acceso basado en roles y autenticación multifactorial.
c) Cifrado de nivel militar en tránsito y en reposo.
2) Detección
a) Mitigación de amenazas desde el borde hasta el núcleo y la nube
b) Infraestructura completa y visibilidad de datos.
c) Detección de anomalías impulsada por IA y escaneo automatizado de malware.

3) Recuperación
a) Recuperación orquestada y automatizada a escala
b) Visibilidad de las últimas copias de seguridad libres de malware en buen estado
c) Recuperación limpia y sin rescate

El postor deberá realizar al menos una prueba de recuperación de la información durante el periodo que dure el soporte. Asimismo, se tendrá soporte de la marca para casos de fallo de hardware incluyendo la autorización de retorno de mercadería (RMA).

El Postor deberá reconfigurar la integración entre las soluciones veritas que se encuentran disponibles en distintas ubicaciones o sedes de la Fuerza Aérea del Perú a fin de asegurar que las ultimas copias de seguridad se encuentren respaldadas y replicadas de forma correcta.

En el soporte estará contemplado la escalación de casos con el fabricante y la devolución de mercancía (RMA) en caso presente un algún imprevisto o error que este fuera del soporte local. Como parte de los entregables el proveedor deberá remitir el certificado expedido por la marca para la extensión del soporte y garantía desde 22-07-2024 hasta 31-10-2025. A partir de 01-11-2025 hasta el 31-12-2025 el postor deberá asegurar la disponibilidad del servicio con una solución alterna de la misma marca en modo stand alone con similares funcionalidades técnicas, solamente en el caso fortuito que el Veritas NetBackup 5240 presente alguna falla de hardware y software que impida su funcionamiento.

c.- **Extensión de suscripción de licencias, soporte de fábrica de hardware y software del Firewall CheckPoint 5600.**

La institución cuenta con dos (2) equipos que se encuentran en alta disponibilidad (HA) del fabricante CheckPoint modelo 5600 con licenciamiento de tipo prevención de amenazas de próxima generación y SandBlast (NGTX). Esta licencia permite contar con las siguientes características:

1) Funcionalidades de Red
a) La solución debe ser capaz de operar en modalidad Layer 3 (routing), modalidad in-line (bridge) y L2 (port mirroring y/o monitor mode).
b) Deben soportar inspección del tráfico cifrado (SSL/HTTPS).
c) Debe soportar enrutamiento con IPv4 e IPv6.
d) Debe soportar DHCP en modos: Servidor DHCP y DHCP Relay (reenvío) en IPv4 e IPv6.
e) Debe soportar control de ancho de banda basado en prioridades de pesos.
f) Debe poder realizar límites de ancho de banda (upload/download) para controlar tráfico por tipo de destino, servicio y/o aplicación.
g) Soporte de rutas estáticas, PBR (policy based routing), LACP, OSPF (IPv4 e IPv6), RIP, BGP, IGMP, PIM, Ipsec Routing y Dual Stack IPv4 e IPv6, NAT64, NAT46 y NAT66.
h) La solución soporta ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
i) El soporte a políticas de ruteo permite que, ante la presencia de dos enlaces, se pueda decidir por que enlace egresa tráfico determinado.
j) La solución debe soportar políticas de ruteo estático en IPv6.
k) La solución debe soportar registro de tablas ARP estáticas y dinámicas, definiendo cantidad de entradas ARP y el tiempo de duración.
l) Debe incluir la posibilidad de crear NAT permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete y en una sola regla.

2) Gestión de políticas
a) El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como direcciones IP, redes, usuarios, grupos de usuarios, servicios de red, comunidad de VPN, direcciones de URL y aplicaciones.
b) Sobre la base de las políticas creadas debe tener capacidad de habilitar diversas acciones tales como: Accept, Drop, Reject, Limit (limitar ancho de banda) y habilitar autenticación de usuario final.
c) Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
d) Las reglas del firewall deben tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando.
e) Las reglas de firewall deben poder tener limitantes y/o vigencia en base a tiempo o determinado período (día, mes, año, día de la semana y hora).
f) Debe tener capacidad de crear reglas de firewall en base a objetos dinámicos, los cuales son basados en fuentes de URL externas (HTTP/HTTPs) que contengan archivos CSV o Json, con la finalidad de automatizar las reglas de acceso, no siendo necesario publicar y/o compilar reglas en el firewall.

3) Geolocalización
a) Soportar la creación de políticas basada en Geolocalización, configurando que el tráfico de determinado País y/o Países sean bloqueados o permitidos.

b) Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.
c) Debe posibilitar la creación de bloqueo general de diversos países desde la interfaz gráfica y crear de excepciones utilizando políticas.
d) Las actualizaciones de las direcciones o rangos de IP publica por cada país, debe realizarse periódicamente y de manera automática.

4) Prevención de Intrusos – IPS

a) La solución debe proveer un sistema de prevención de intrusos (IPS) integrado a la solución de seguridad.
b) El IPS debe contar con mecanismo de detección de amenazas de múltiples niveles o métodos: detección por firmas en vulnerabilidades, validación de protocolos, detección de anomalías, detección basada en comportamiento.
c) Debe tener protección contra ataques DoS (Denial of Service).
d) A nivel de aplicación, debe incluir protecciones tipo Cross Site Scripting, SQL Injection, Command Injection e injection protecction para DN (Distinguished Names).
e) El IPS debe proveer al menos dos políticas o perfiles precargados, para ser usados inmediatamente.
f) Las firmas de protección de IPS deben poder categorizarse según un nivel de severidad, nivel de efectividad (confianza) y nivel consumo de recursos.
g) Por cada protección o por todas las protecciones soportadas, debe permitir adicionar excepciones basadas en objetos de red o mediante las reglas de seguridad configuradas.
h) Debe poder realizar captura de paquetes para protecciones específicas.
i) Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: HTTP, SMTP, IMAP, DNS tunneling, FTP, SNMP, IMAP, SMB.
j) Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos.
k) Debe detectar y bloquear intentos de túneles, a fin de evitar fuga de datos o problemas de seguridad web.
l) Debe proteger contra ataques tipo DNS Cache Poisoning cuando reutilizan los puertos de origen.
m) Debe soportar Inspección de tráfico encriptado HTTPS tanto Inbound como Outbound.
n) La solución debe tener capacidades de detección y prevención de ataques tunelizados en tráfico DNS.
o) Debe permitir adicionar excepciones a las protecciones de IPS desde el log o de manera manual.
p) Debe poder capturar paquetes automáticamente de eventos de IPS, para proveer un mejor análisis forense.
q) La funcionalidad de IPS debe tener las siguientes capacidades:
r) Detección y prevención de vulnerabilidades, incluidas herramientas de explotación conocidas y desconocidas, y protección contra CVE específicos.
s) Detección y prevención del uso indebido de un protocolo, para actividad maliciosa o amenaza potencial.
t) Detección y prevención de comunicaciones de malware salientes.
u) Detección y prevención de intentos de tunelización, para intentos de fuga de datos o intentos de eludir otras medidas de seguridad, como el filtrado web.
v) Detección, prevención o restricción de ciertas aplicaciones que pueden causar amenazas a la seguridad de la red, como las aplicaciones P2P o de mensajería instantánea.

5) Anti-Bot o Antispyware

a) La solución debe proveer una herramienta que haga descubrimiento de “bots” dentro de la red. Dicha herramienta debe bloquear la comunicación que intenten establecer los equipos infectados “bots” hacia las redes de los atacantes en Internet (botnet).
b) La solución debe incluir al menos los siguientes métodos de identificación:
c) Identificación de direcciones web de Comando y Control utilizadas por los criminales para controlar los bots.
d) Identificación de patrones (fingerprints) de comunicación utilizada por cada familia de bots.
e) Identificación de comportamiento de bots.
f) La solución debe contar con un repositorio en la nube del propio fabricante para la identificación de direcciones y patrones de comunicación de “botnet”. El Anti-Bot se debe actualizar continuamente de manera automática.
g) La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de direcciones IP, URL y recursos DNS no identificados y/o no clasificados.
h) La solución debe tener una capa de protección DNS, para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA), empleando protección basada en Machine Learning, así como protección fuga o exfiltración de información mediante DNS Tunneling.
i) La solución debe contar con análisis la reputación de direcciones URL, direcciones IP y los dominios externos (DNS) a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C).

6) Control de aplicaciones y Filtro de URL

a) La solución debe ser capaz de identificar, permitir o bloquear aplicaciones y páginas Web.

b) Se requiere que la detección de aplicaciones sea basada en APP-ID (decodificación de protocolos y aplicaciones, junto a detección heurística), o en base a firmas. En el caso que la solución sea basada en firmas, la base de datos de control de aplicaciones debe contener al menos 10,000 aplicaciones.
c) La base de datos de control de aplicaciones debe actualizarse por un servicio basado en la nube, la actualización debe ser periódica y automática.
d) Debe permitir la creación de firmas personalizadas para el Control de Aplicaciones y URL Filtering, mediante herramientas del propio del fabricante.
e) Debe alertar al usuario cuando una aplicación o página web fuera bloqueada.
f) Solución debe soportar como mínimo 100 categorías de URL Filtering, que incluya categorías para protección de riesgo informático, tales como: Phishing, SPAM, Botnets, Anonymizer, Hacking, Inactive Sites y Spyware/ Malicious Sites.
g) La solución debe proveer una librería de aplicaciones que incluya aplicaciones Web 2.0, Widgets y base de datos de URL.
h) Debe ser posible definir nuevas aplicaciones y sitios web, así como categorías y grupos que no estén definidos dentro de la base de datos.
i) Debe ser posible permitir o bloquear aplicaciones o sitios al menos por los siguientes parámetros: Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales (usuarios) y grupos de usuarios.
j) La solución debe categorizar las aplicaciones y URLs por factor de riesgo.
k) Debe ser posible definir la política de seguridad de aplicaciones y URLs basada en identidades de usuario.
l) La solución debe proporcionar un mecanismo para limitar el uso de aplicaciones basadas en el consumo de ancho de banda (upload / download) por el tipo de aplicación y/o servicio de red definido.
m) Solución debe inspeccionar el tráfico web cifrado (SSL/TLS) de los usuarios, y permitir excepciones granulares de inspección para proteger la privacidad de los usuarios y/o cumplir con regulaciones.
n) Debe permitir la categorización de los sitios HTTPS basado en el contenido del campo SNI (Server Name Indication), sin la necesidad de descifrar el tráfico web.
o) Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y soportar protección al protocolo HTTP/2.
p) Debe soportar la inspección de tráfico HTTPS sobre puertos no estándar (distinto a los puertos HTTP/HTTPS).

7) Prevención de amenazas

a) Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en el repositorio la clasificación y/o reputación de direcciones IP, Dominios, URL, redes de Comando y Control y ataques DoS.
b) Debe tener capacidad de clasificación y análisis de archivos y posterior validación en el repositorio de inteligencia de amenazas en nube del propio fabricante, sin generar un impacto en el rendimiento de la red.
c) Los equipos deben tener integrada la detección y prevención de virus y amenazas (antimalware).
d) La inspección de archivos y prevención de amenazas debe ser en el tráfico entrante y saliente.
e) Debe tener capacidad de protección de pre-infección del malware que fue identificado en los archivos.
f) Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web (HTTP, HTTPS), Mail (SMTP o POP3), SMB y FTP.
g) Debe prevenir infección de archivos maliciosos (Word, Excel, PowerPoint, PDF) en tiempo real.
h) Debe tener una base de datos local de firmas de malware y cache de reputación de URL, para una respuesta rápida. Si una URL no está ubicada en la cache, debe ser consultada automáticamente en el repositorio de Inteligencia de amenazas en nube para su clasificación y prevención.
i) Debe soportar Inspección de tráfico cifrado/encriptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).
j) Debe impedir la descarga de malware desde Internet, impidiendo el acceso a sitios que se sabe que relacionados con Malware.
k) Debe tener capacidades de inspección y prevención de amenaza en el canal cifrado SSH, con las siguientes capacidades:
l) Bloquear ataques en canal SSH.
m) Bloquea la transmisión de virus a través de los protocolos SCP y SFTP.
n) Prevenir el descifrado de contraseñas en fuerza bruta de servidores SSH/SFTP.
o) Prevenir el reenvío de puertos SSH (Port Forwarding).
p) Prevenir el uso de criptografía vulnerable en el canal SSH.
q) Prevenir el uso de clientes y servidores SSH vulnerables.
r) Prevenir el uso del puerto 22 para otros protocolos que no sean SSH.
s) Debe soportar el manejo personalizado (añadir, borrar o modificar) para la alimentación de IoC (Indicadores de Compromiso), en formato CSV y Structured Threat Information Expression (STIX XML).
t) Debe tener capacidad de integración con fuente de IoC de terceros (External IoC) a través de

direcciones web URL, con capacidades de detección y prevención. La aplicación y prevención de seguridad, en base a los IoC incluidos, debe ser de manera automática, sin interacción del usuario administrador.

8) Prevención de amenazas desconocidas o de día-cero (Emulación y Extracción de malware)

a) La solución debe ser capaz de identificar y prevenir ataques y malware no conocido, presentes en documentos y/o archivos ejecutables.
b) La solución debe ser capaz de emular los archivos identificados en el firewall de forma automática, a través del envío y posterior análisis en la nube del propio fabricante de la solución de firewall para la Emulación de Malware (sandbox).
c) La solución debe proteger a los usuarios internos, de manera que prevenga el acceso o descarga a los archivos en tanto estos son analizados en el equipo de emulación, si el archivo es benigno se entrega el archivo original al usuario y si el archivo es maligno se deniega su acceso o descarga.
d) La solución debe proporcionar la capacidad de protección contra ataques de malware desconocido y de día cero antes de que se hayan creado protecciones de firmas estáticas.
e) La solución debe proveer prevención en tiempo real de malware desconocido en las descargas web y canal de correo electrónico.
f) La solución deberá poder emular archivos para la identificación de malware que viajan en los protocolos: HTTP, HTTPS, SMTP, IMAP, CIFS, SMBv3, SMBv3 multi-channel y FTP.
g) La solución deberá poder emular al menos los siguientes tipos de archivos: Adobe PDF, Microsoft Office (documentos y plantillas), DLL, Java, Flash, Scripts, archivos comprimidos (ZIP, 7Z, RAR, GZ, TGZ, TAR, TAR.GZ y JAR), ejecutables (EXE, COM, LNK, DLL, DRV, SYS, SCR, VBX) y archivos de MacOS (APP, DMG, PKG).
h) Cada archivo emulado en el sandbox debe generar un reporte detallado que incluya información forense sobre la actividad maliciosa originada por el archivo, basado en las técnicas y tácticas del framework de ciberseguridad MITRE ATT&CK.
i) El motor de emulación debe detectar llamadas API, cambios en el sistema de archivos, cambios en el registro, conexiones de red, procesos de sistema.
j) El motor de emulación debe admitir varios sistemas operativos, como Windows XP, Windows7, Windows 10 y Windows 11.
k) Las soluciones deben admitir motores de detección automatizados basados en machine learning.
l) La solución debe ser capaz de soportar escaneo de enlaces (links) dentro de correos para detección de malware.
m) La solución debe ser resistente a los casos en los que el código de shell o el malware no se ejecutarían si detectaran la existencia de un entorno virtual.
n) La solución deberá tener capacidad de extracción de amenazas o CDR (Content Disarm Reconstruction), en las descargas de archivos desde Internet inclusive sobre canal cifrado HTTPS para prevenir el riesgo al interior de la red corporativa. Debe tener la capacidad de limpiar archivo durante su análisis, extrayendo el componente activo de riesgo o malicioso que encuentran dentro de los archivos, y, además, poder transformar el archivo en un formato PDF. Esta funcionalidad debe soportar como mínimo los siguientes tipos de archivo para el canal web y correo:

a. Microsoft Excel (XLS, XLSX, XLSB, XLSM, XLTX, SLTM)
b. Microsoft Word (DOC, DOCX, DOCM, DOTX, DOTM, DOT)
c. Microsoft Power Point (PPT, PPS, PPTX, PPTM, POTX, POTM, PPSX) Adobe PDF (PDF, FDF)

o) Así mismo, la capacidad de extracción y/o transformación de los archivos para prevención de amenazas, debe ser efectuada a los archivos adjuntos en canal de correo (modo MTA) para los formatos: Imágenes (JPEG, JPG, BMP, PSD, GIF, TIF, PNG) XML, TXT. HTML, JS.
p) La extracción de malware deberá retirar los componentes de riesgo de los documentos tales como: Macros, Objetos Embebidos, Enlaces (Linked Objects), PDF JavaScripts y PDF Launch.

9) Identificación de usuarios

La solución debe proveer diferentes métodos para obtener las identidades de los usuarios, tales como:

a) Sin agente, haciendo búsquedas al Directorio Activo Microsoft.
b) Con agente implementado en los servidores de Directorio Activo Microsoft.
c) Empleando un Portal Cautivo.
d) Empleando un Proveedor de Indentidad (IdP) basado en SAML.
e) La solución debe soportar el uso del protocolo WMI (Windows management instrumentation).
f) La solución debe soportar el uso del protocolo Kerberos (Transparent Kerberos Authentication).
g) Debe proveer un “Portal Cautivo”, para autentificar a los usuarios que no están dentro del Directorio Activo, los usuarios que no tienen plataforma Windows y/o los usuarios invitados.
h) La solución debe proveer configuración de acceso basado reglas de tiempo, en las cuales los usuarios puedan entrar a los recursos de la red.
i) Cuando se detecte que los usuarios no se han autenticado, la solución tiene que redireccionarlos a un Portal Cautivo, a través del protocolo HTTP.
j) Debe soportar al menos los siguientes métodos de autenticación: nombre de usuario y contraseña, que podrá ser configurado en la base de dates Interna del equipo, servidor de LDAP y servidor de RADIUS.

k) La solución debe retener la identidad de los usuarios aun cuando estos cambien la dirección IP.
l) La solución debe integrarse con el Directorio Activo Microsoft sin la necesidad de instalar un agente en el Servidor de Dominio o en los equipos de los usuarios finales.
m) La solución debe integrarse con el servicio de Azure AD (Microsoft) para la autenticación y autorización de usuarios en las reglas de acceso del firewall.

10) VPN Ipsec

a) Debe soportar IPSec VPN (Client-to-Site y Site-to-Site) y capacidad de usuarios ilimitada o hasta el de usuarios que permita la capacidad del equipo.
b) Debe soportar túneles VPN punto a punto (Site-to-Site) y túneles de acceso remoto para usuario final (Client-to-Site).
c) Los siguientes esquemas de autenticación deben ser soportados por los módulos de firewall y VPN: Tokens (Ejemplo: SecureID), TACACS, RADIUS y Certificados Digitales.
d) Debe permitir almacenar una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo.
e) Deben ser soportados 3DES y AES-256 para las fases I y II de IKE.
f) Debe soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).
g) Debe soportar integridad de datos con MD5 y SHA1.
h) Debe incluir soporte a las topologías VPNs site-to-site: Todos a todos, Oficinas Remotas a Sitio Central y Sitio remoto a través del sitio central hacia otro sitio remoto.
i) Soporte a VPNs client-to-site basadas en IPSEC.
j) Debe poder establecer VPNs con Firewalls con direcciones IP dinámicas públicas o resolución de DNS.
k) Debe poder integrarse con Directorio Activo Microsoft u Open LDAP para crear reglas de control de acceso a través de VPN, empleando: usuarios, grupos de usuarios, maquinas, dirección IP y redes.
l) Debe poder integrarse con Azure AD (Microsoft) mediante SAML para autenticación en el acceso remoto de clientes VPN.
m) El cliente VPN, debe instalarse sobre sistemas operativos Windows, Linux y MacOS.
n) La solución debe contar con autenticación de doble factor mediante el certificado del cliente y el usuario/contraseña.
o) La solución VPN, debe ser capaz de evaluar la configuración del dispositivo cliente antes de otorgar el acceso a la red corporativa, por lo menos las siguientes condiciones:
1. Verificar el sistema operativo.
2. Verifica si el usuario logeado en el equipo es miembro de grupos específicos.
3. Verifica si procesos específicos se están ejecutando o no.
4. Verifica las llaves de registro, valores y su contenido.
5. Verifica el hardware de CPU, tipo y modelo.
6. Verifica los componentes de Windows Security Center, se puede elegir que componente y si es que están instalados y ejecutándose.

11) QoS

Debe contar con un módulo integrado de Calidad de Servicio o QoS, que permita principalmente:

a) Priorización de tráfico crítico para el negocio, sobre el tráfico de menor prioridad (no critico).
b) Garantice el ancho de banda y controlador de la latencia para aplicaciones de transmisión, como son Voz sobre IP (VoIP) y videoconferencia.
c) Otorgue acceso garantizado o prioritario a empleados específicos, incluso si acceden de forma remota a los recursos de la red.
d) El QoS debe permitir la definición:
   1. Porcentaje del ancho de banda disponible, basado en prioridad de regla.
   2. Ancho de banda mínimo garantizado
   3. Ancho de banda máximo, basado en limites
e) Deberá permitir aplicar reglas de QoS para el tráfico cifrado de VPN.
f) Debe tener capacidad de QoS Queuing para servicio de baja latencia (Low Latency) para poder definir clases especiales de servicio para aplicaciones "sensibles a demoras" como voz y video.

La extensión de licencia incluye la suscripción Annuity Blades que dan acceso continuo para actualizaciones de seguridad que permitirá la optimización de las diversas funcionalidades del equipo CheckPoint 5600.; Asimismo, la apertura y manejo de casos con la marca CheckPoint mediante su portal y la autorización de devolución de mercancía (RMA) en caso presente algún imprevisto o error que no sea solucionable por el soporte del Postor. Como parte de los entregables el proveedor tiene que emitir el certificado expedido por la marca para la renovación de suscripción de licencia y la extensión del soporte y garantía desde 28-11-2024 hasta 31-12-2025.

d.- **Extensión de suscripción de licencias, soporte de fábrica de hardware y software del Firewall CheckPoint 5900**

La FAP cuenta con dos (2) equipos que se encuentran en HA del fabricante CheckPoint modelo 5900 con licenciamiento Next Generation Threat Prevention (NGTP). Esta licencia debe incluir:

1) **Funcionalidades de Red**

a) La solución debe ser capaz de operar en modalidad Layer 3 (routing), modalidad in-line (bridge) y L2 (port mirroring y/o monitor mode).
b) Deben soportar inspección del tráfico cifrado (SSL/HTTPS).
c) Debe soportar enrutamiento con IPv4 e IPv6.
d) Debe soportar DHCP en modos: Servidor DHCP y DHCP Relay (reenvío) en IPv4 e IPv6.
e) Debe soportar control de ancho de banda basado en prioridades de pesos.
f) Debe poder realizar límites de ancho de banda (upload/download) para controlar tráfico por tipo de destino, servicio y/o aplicación.
g) Soporte de rutas estáticas, PBR (policy based routing), LACP, OSPF (IPv4 e IPv6), RIP, BGP, IGMP, PIM, Ipsec Routing y Dual Stack IPv4 e IPv6, NAT64, NAT46 y NAT66.
h) La solución soporta ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
i) El soporte a políticas de ruteo permite que, ante la presencia de dos enlaces, se pueda decidir por que enlace egresa tráfico determinado.
j) La solución debe soportar políticas de ruteo estático en IPv6.
k) La solución debe soportar registro de tablas ARP estáticas y dinámicas, definiendo cantidad de entradas ARP y el tiempo de duración.
l) Debe incluir la posibilidad de crear NAT permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete y en una sola regla.

2) Gestión de políticas

a) El equipo debe permitir la creación de políticas de acceso y de prevención de amenazas, con capacidad de seleccionar campos como direcciones IP, redes, usuarios, grupos de usuarios, servicios de red, comunidad de VPN, direcciones de URL y aplicaciones.
b) Sobre la base de las políticas creadas debe tener capacidad de habilitar diversas acciones tales como: Accept, Drop, Reject, Limit (limitar ancho de banda) y habilitar autenticación de usuario final.
c) Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
d) Las reglas del firewall deben tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando.
e) Las reglas de firewall deben poder tener limitantes y/o vigencia en base a tiempo o determinado período (día, mes, año, día de la semana y hora).
f) Debe tener capacidad de crear reglas de firewall en base a objetos dinámicos, los cuales son basados en fuentes de URL externas (HTTP/HTTPs) que contengan archivos CSV o Json, con la finalidad de automatizar las reglas de acceso, no siendo necesario publicar y/o compilar reglas en el firewall.

3) Otras funcionalidades

a) Administración accesible a través de SSH y de interfaz Web segura (HTTPS).
b) La herramienta debe ser capaz de realizar backup/restore de la configuración, permitiendo al administrador programar la realización de los backups (configuración del sistema operativo) en el tiempo deseado.
c) Los backups pueden ser almacenados localmente y el administrador puede transferirlos vía FTP, TFTP y SCP de manera programada.
d) La comunicación entre los servidores de administración y el equipo de seguridad (firewall), debe ser cifrada y autenticada.
e) Debe tener la opción de negar los parámetros de origen o destino, es decir que para una regla dada permite todas las conexiones de origen / destino excepto la especificada en la regla.
f) La solución debe permitir integración con analizadores de tráfico mediante el protocolo NetFlow.
g) Integración mediante API REST de Terceros.
h) Los firewalls deben permitir manejo de ancho de banda de distintos protocolos y/o aplicaciones, permitiendo la definición de niveles de ancho de banda tanto para carga (upload) y descarga (download).
i) Debe soportar y proteger protocolos de VoIP (SIP, H.323, MGCP, SCCP) incluyendo soporte de NAT para cada uno de esos protocolos.

4) Prevención de Intrusos – IPS

a) La solución debe proveer un sistema de prevención de intrusos (IPS) integrado a la solución de seguridad.
b) El IPS debe contar con mecanismo de detección de amenazas de múltiples niveles o métodos: detección por firmas en vulnerabilidades, validación de protocolos, detección de anomalías, detección basada en comportamiento.
c) Debe tener protección contra ataques DoS (Denial of Service).
d) A nivel de aplicación, debe incluir protecciones tipo Cross Site Scripting, SQL Injection, Command Injection e injection protecction para DN (Distinguished Names).
e) El IPS debe proveer al menos dos políticas o perfiles precargados, para ser usados inmediatamente.
f) Las firmas de protección de IPS deben poder categorizarse según un nivel de severidad, nivel

de efectividad (confianza) y nivel consumo de recursos.
g) Por cada protección o por todas las protecciones soportadas, debe permitir adicionar excepciones basadas en objetos de red o mediante las reglas de seguridad configuradas.
h) Debe poder realizar captura de paquetes para protecciones específicas.
i) Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: HTTP, SMTP, IMAP, DNS tunneling, FTP, SNMP, IMAP, SMB.
j) Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos.
k) Debe detectar y bloquear intentos de túneles, a fin de evitar fuga de datos o problemas de seguridad web.
l) Debe proteger contra ataques tipo DNS Cache Poisoning cuando reutilizan los puertos de origen.
m) Debe soportar Inspección de tráfico encriptado HTTPS tanto Inbound como Outbound.
n) La solución debe tener capacidades de detección y prevención de ataques tunelizados en tráfico DNS.
o) Debe permitir adicionar excepciones a las protecciones de IPS desde el log o
p) de manera manual.
q) Debe poder capturar paquetes automáticamente de eventos de IPS, para proveer un mejor análisis forense.
r) La funcionalidad de IPS debe tener las siguientes capacidades:
s) Detección y prevención de vulnerabilidades, incluidas herramientas de explotación conocidas y desconocidas, y protección contra CVE específicos.
t) Detección y prevención del uso indebido de un protocolo, para actividad maliciosa o amenaza potencial.
u) Detección y prevención de comunicaciones de malware salientes.
v) Detección y prevención de intentos de tunelización, para intentos de fuga de datos o intentos de eludir otras medidas de seguridad, como el filtrado web.
w) Detección, prevención o restricción de ciertas aplicaciones que pueden causar amenazas a la seguridad de la red, como las aplicaciones P2P o de mensajería instantánea.

5) Anti-Bot o Antispyware

a) La solución debe proveer una herramienta que haga descubrimiento de “bots” dentro de la red. Dicha herramienta debe bloquear la comunicación que intenten establecer los equipos infectados “bots” hacia las redes de los atacantes en Internet (botnet).
b) La solución debe incluir al menos los siguientes métodos de identificación:
a. Identificación de direcciones web de Comando y Control utilizadas por los criminales para controlar los bots.
b. Identificación de patrones (fingerprints) de comunicación utilizada por cada familia de bots.
c. Identificación de comportamiento de bots.
c) La solución debe contar con un repositorio en la nube del propio fabricante para la identificación de direcciones y patrones de comunicación de “botnet”. El Anti-Bot se debe actualizar continuamente de manera automática.
d) La solución debe contar con un repositorio en nube del fabricante que permita realizar consultas de direcciones IP, URL y recursos DNS no identificados y/o no clasificados.
e) La solución debe tener una capa de protección DNS, para protección contra dominios maliciosos de malware basados en Algoritmos de Generación de Dominio (DGA), empleando protección basada en Machine Learning, así como protección fuga o exfiltración de información mediante DNS Tunneling.
f) La solución debe contar con análisis la reputación de direcciones URL, direcciones IP y los dominios externos (DNS) a los que acceden los equipos en la red, para identificar y prevenir actividad conocida o sospechosa, como Command and Control (C&C).

6) Control de aplicaciones y Filtro de URL

a) La solución debe ser capaz de identificar, permitir o bloquear aplicaciones y páginas Web.
b) Se requiere que la detección de aplicaciones sea basada en APP-ID (decodificación de protocolos y aplicaciones, junto a detección heurística), o en base a firmas. En el caso que la solución sea basada en firmas, la base de datos de control de aplicaciones debe contener al menos 10,000 aplicaciones.
c) La base de datos de control de aplicaciones debe actualizarse por un servicio basado en la nube, la actualización debe ser periódica y automática.
d) Debe permitir la creación de firmas personalizadas para el Control de Aplicaciones y URL Filtering, mediante herramientas del propio del fabricante.
e) Debe alertar al usuario cuando una aplicación o página web fuera bloqueada.
f) Solución debe soportar como mínimo 100 categorías de URL Filtering, que incluya categorías para protección de riesgo informático, tales como: Phishing, SPAM, Botnets, Anonymizer, Hacking, Inactive Sites y Spyware/ Malicious Sites.
g) La solución debe proveer una librería de aplicaciones que incluya aplicaciones Web 2.0, Widgets y base de datos de URL.
h) Debe ser posible definir nuevas aplicaciones y sitios web, así como categorías y grupos que no estén definidos dentro de la base de datos.
i) Debe ser posible permitir o bloquear aplicaciones o sitios al menos por los siguientes parámetros:

Aplicación Individual, URL o aplicación, categorías, niveles de riesgo, reglas individuales (usuarios) y grupos de usuarios.

j) La solución debe categorizar las aplicaciones y URLs por factor de riesgo.
k) Debe ser posible definir la política de seguridad de aplicaciones y URLs basada en identidades de usuario.
l) La solución debe proporcionar un mecanismo para limitar el uso de aplicaciones basadas en el consumo de ancho de banda (upload / download) por el tipo de aplicación y/o servicio de red definido.
m) Solución debe inspeccionar el tráfico web cifrado (SSL/TLS) de los usuarios, y permitir excepciones granulares de inspección para proteger la privacidad de los usuarios y/o cumplir con regulaciones.
n) Debe permitir la categorización de los sitios HTTPS basado en el contenido del campo SNI (Server Name Indication), sin la necesidad de descifrar el tráfico web.
o) Debe poder realizar la implementación de TLS 1.3 para inspección de canal cifrado y soportar protección al protocolo HTTP/2.
p) Debe soportar la inspección de tráfico HTTPS sobre puertos no estándar (distinto a los puertos HTTP/HTTPS).

7) Prevención de amenazas

a) Debe utilizar el repositorio de inteligencia de amenazas en nube del propio fabricante, para recibir actualizaciones de firmas y consultar en el repositorio la clasificación y/o reputación de direcciones IP, Dominios, URL, redes de Comando y Control y ataques DoS.
b) Debe tener capacidad de clasificación y análisis de archivos y posterior validación en el repositorio de inteligencia de amenazas en nube del propio fabricante, sin generar un impacto en el rendimiento de la red.
c) Los equipos deben tener integrada la detección y prevención de virus y amenazas (anti-malware).
d) La inspección de archivos y prevención de amenazas debe ser en el tráfico entrante y saliente.
e) Debe tener capacidad de protección de pre-infección del malware que fue identificado en los archivos.
f) Deberá realizar análisis de malware y bloquearlos en al menos los siguientes protocolos: Web (HTTP, HTTPS), Mail (SMTP o POP3), SMB y FTP.
g) Debe prevenir infección de archivos maliciosos (Word, Excel, PowerPoint, PDF) en tiempo real.
h) Debe tener una base de datos local de firmas de malware y cache de reputación de URL, para una respuesta rápida. Si una URL no está ubicada en la cache, debe ser consultada automáticamente en el repositorio de Inteligencia de amenazas en nube para su clasificación y prevención.
i) Debe soportar Inspección de tráfico cifrado/encriptado sobre protocolo HTTPS, tanto tráfico entrante (Inbound), como tráfico saliente (Outbound).
j) Debe impedir la descarga de malware desde Internet, impidiendo el acceso a sitios que se sabe que relacionados con Malware.
k) Debe tener capacidades de inspección y prevención de amenaza en el canal cifrado SSH, con las siguientes capacidades:
l) Bloquear ataques en canal SSH.
m) Bloquea la transmisión de virus a través de los protocolos SCP y SFTP.
n) Prevenir el descifrado de contraseñas en fuerza bruta de servidores SSH/SFTP.
o) Prevenir el reenvío de puertos SSH (Port Forwarding).
p) Prevenir el uso de criptografía vulnerable en el canal SSH.
q) Prevenir el uso de clientes y servidores SSH vulnerables.
r) Prevenir el uso del puerto 22 para otros protocolos que no sean SSH.
s) Debe soportar el manejo personalizado (añadir, borrar o modificar) para la alimentación de IoC (Indicadores de Compromiso), en formato CSV y Structured Threat Information Expression (STIX XML).
t) Debe tener capacidad de integración con fuente de IoC de terceros (External IoC) a través de direcciones web URL, con capacidades de detección y prevención. La aplicación y prevención de seguridad, en base a los IoC incluidos, debe ser de manera automática, sin interacción del usuario administrador.

8) Identificación de usuarios

a) La solución debe proveer diferentes métodos para obtener las identidades de los usuarios, tales como:
b) Sin agente, haciendo búsquedas al Directorio Activo Microsoft.
c) Con agente implementado en los servidores de Directorio Activo Microsoft.
d) Empleando un Portal Cautivo.
e) Empleando un Proveedor de Indentidad (IdP) basado en SAML.
f) La solución debe soportar el uso del protocolo WMI (Windows management instrumentation).
g) La solución debe soportar el uso del protocolo Kerberos (Transparent Kerberos Authentication).
h) Debe proveer un “Portal Cautivo”, para autentificar a los usuarios que no están dentro del Directorio Activo, los usuarios que no tienen plataforma Windows y/o los usuarios invitados.
i) La solución debe proveer configuración de acceso basado reglas de tiempo, en las cuales los

usuarios puedan entrar a los recursos de la red.

j) Cuando se detecte que los usuarios no se han autenticado, la solución tiene que redireccionarlos a un Portal Cautivo, a través del protocolo HTTP.
k) Debe soportar al menos los siguientes métodos de autenticación: nombre de usuario y contraseña, que podrá ser configurado en la base de dates Interna del equipo, servidor de LDAP y servidor de RADIUS.
l) La solución debe retener la identidad de los usuarios aun cuando estos cambien la dirección IP.
m) La solución debe integrarse con el Directorio Activo Microsoft sin la necesidad de instalar un agente en el Servidor de Dominio o en los equipos de los usuarios finales.
n) La solución debe integrarse con el servicio de Azure AD (Microsoft) para la autenticación y autorización de usuarios en las reglas de acceso del firewall.

9) QoS

a) Debe contar con un módulo integrado de Calidad de Servicio o QoS, que permita principalmente:
   1. Priorización de tráfico crítico para el negocio, sobre el tráfico de menor prioridad (no critico).
   2. Garantice el ancho de banda y controlar la latencia para aplicaciones de transmisión, como son Voz sobre IP (VoIP) y videoconferencia.
   3. Otorgue acceso garantizado o prioritario a empleados específicos, incluso si acceden de forma remota a los recursos de la red.

b) El QoS debe permitir la definición:
1. Porcentaje del ancho de banda disponible, basado en prioridad de regla.
2. Ancho de banda mínimo garantizado
3. Ancho de banda máximo, basado en limites

c) Deberá permitir aplicar reglas de QoS para el tráfico cifrado de VPN.
d) Debe tener capacidad de QoS Queuing para servicio de baja latencia (Low Latency) para poder definir clases especiales de servicio para aplicaciones "sensibles a demoras" como voz y video.

La extensión de licencia incluye la suscripción Annuity Blades que dan acceso continuo para actualizaciones de seguridad que permitirá la optimización de las diversas funcionalidades del equipo CheckPoint 5900. Asimismo, debe incluir la apertura de nuevos casos con soporte de la marca e incluir en caso fuese necesario la autorización de devolución de mercancía (RMA). Como parte de los entregables el proveedor deberá remitir el certificado expedido por la marca para la renovación de suscripción de licencia y la extensión del soporte y garantía desde 28-11-2024 hasta 31-12-2025.

e.- **Extensión de Suscripción de Licencias, soporte de fábrica de hardware y software del Checkpoint Sandblast. TE-1000X**

La extensión de licencia y soporte deberá contar con las siguientes características:

1) EMULACIÓN DE AMENAZA

a) Entornos de emulación
   a) PC: Windows XP o posterior
   b) Mac: MacOS versión 10.14.6 (Mojave) o posterior
b) Tipos de archivos Más de 70 tipos de archivos emulados, incluidos: documentos y plantillas de Microsoft Office, EXE, DLL, Archivos (ISO, ZIP, 7Z, RAR, etc.), PDF, Flash, Java, scripts y más.
c) Archivar archivos archivados (comprimidos)
d) Archivos protegidos con contraseña

2) EXTRACCIÓN DE AMENAZA

a) Tipos de archivo

Descargas web y archivos adjuntos de correo electrónico en los siguientes formatos:

i) Microsoft Word
ii) Microsoft PowerPoint
iii) Microsoft Excel
iv) Adobe PDF
v) Archivos de imagen

b) Modos de extracción
   1. Limpiar y mantener el tipo de archivo original
   2. Convertir a PDF

c) Componentes extraíbles

Más de 15 tipos de componentes extraíbles (configurables), que incluyen:

i) Macros y código
ii) Objetos incrustados
iii) Objetos vinculados
iv) Acciones de JavaScript en PDF
v) Acciones de inicio de PDF

La extensión de licencia incluye la suscripción Annuity Blades que dan acceso continuo para actualizaciones de seguridad que permitirá la optimización de las diversas funcionalidades del equipo CheckPoint Sandblast TE-

1000X con herramientas de sandboxing, prevención de intrusiones (IPS), filtrado web, antivirus, antimalware y prevención de perdida de datos (DLP), además la prevención del empleo de herramientas o vulnerabilidades como malware, ataques zero-day, phishing, ataques basados en web o botnets. Asimismo, la apertura de casos con soporte de la marca Checkpoint y autorización de devolución de mercancía (RMA). Como parte de los entregables el proveedor tiene remitir el certificado expedido por la marca para la renovación de suscripción de licencia y la extensión del soporte y garantía desde 28-11-2024 hasta 31-12-2025.

f.- **Extensión de licencia, soporte y garantía de fábrica del Infoblox Trinzic (DNS, DHCP, IPAM)**

El soporte de la presente solución está establecido para el equipo Infoblox modelo Trinzic 1405, el cual incluye la apertura de casos con soporte de Infoblox y autorización de devolución de mercancía (RMA) en caso presente un algún imprevisto o error que lo requiera. Como parte de los entregables el proveedor Deberá remitir el certificado expedido por la marca para la extensión del soporte y garantía desde 08-11-2024 hasta 31-12-2025.

La extensión del soporte y garantía deberá contemplar las capacidades de licencia DDI GD.

1) DNS

DNS autoritativo, DNS recursivo y servicios autoritativos secundarios, grupos de servidores de nombres, actualizaciones de DDNS, envejecimiento y eliminación de registros de DNS, firma y validación de DNSSEC, DNS Anycast, listas de bloqueo y blackholing de DNS, proxy de reenvío de DNS (DFP), compatibilidad con superhost de DNS, vistas de DNS, importación, exportación y transferencias de datos de zona DNS, y compatibilidad con IPv4 e IPv6

2) DHCP

Conmutación por error de DHCP, filtrado de DHCP, huellas dactilares de DHCP, direcciones fijas de DHCP, notificaciones y alertas de DHCP, opciones de DHCP, espacio y rangos de opciones, umbrales de utilización de DHCP, compatibilidad con IPv4 e IPv6 y plantillas de red (direcciones fijas y rangos)

3) IPAM

Importación y exportación de CSV, atributos extensibles y carpetas inteligentes, vDiscovery, descubrimiento de IPAM básico, vistas de red para administración de espacio de direcciones superpuestas, umbrales de utilización de IPAM, visualización y reservas de IPAM y administración de VLAN

4) Red

Flujos de trabajo de aprobación, autenticación: base de datos local, LDAP, RADIUS, Active Directory, SAML y SSO, aprovisionamiento automático, actualizaciones de software automatizadas: centralizadas, grupos y programación, repositorio de licencias centralizado, paneles personalizados, comunicaciones cifradas entre miembros, candidatos a administrador de red (GMC)) para DR y redundancia, ha utilizado el protocolo de redundancia de enrutador virtual (VRRP), copia de seguridad y restauración manual y programada, servidor NTP y cliente NTP, administración fuera de banda, papelera de reciclaje, control de acceso basado en roles (RBAC) seguro, reforzado Dispositivos de hardware y software.

5) API

API web basada en REST (WAPI), API saliente (licencia de ecosistema)

6) Nube pública

Nube de AWS, Nube de Azure y Azure Stack, Soporte de Google Cloud Platform (GCP), Soporte de Oracle Cloud Infrastructure (OCI)

7) Nube privada

Soporte para VMware, Nutanix, Red Hat OpenShift y OpenStack

8) Hipervisores vNIOS

Compatibilidad con VMware ESXi, KVM, Microsoft Hyper-V y Nutanix

9) Acropolis Hypervisor (AHV)

Integración y orquestación de IPAM, Ansible Collection, Calm (de terceros), Docker, Kubernetes (API), OpenStack, Terraform, VMware, NIOS Grid Connector (ver datos DDI en la nube) y dispositivos Infoblox de Cloud Platform (CP)

10) Loggin

Registros de cara al cliente (descargar y ver), reenvío de registros a las instalaciones (a través de CDC), captura de registros DNS/DHCP de Microsoft, visualización interna de Syslog y reenvío a Syslog remoto

g.- **Extensión de soporte y garantía de fábrica hardware y software del balanceador de carga/SSL A10 Thunder 3030s**

El soporte de la presente solución está establecido para el modelo Thunder 3030S que cuenta con 1xCPU, 6xGoC, 2xGF, 4x10GF, 16 GB de memoria RAM, almacenamiento SSD, distribución de carga alta y baja, configuración de certificados SSL y validación FIPS.

La extensión de soporte y garantía contemplará las siguientes capacidades del equipo:

1) Entrega de aplicaciones

a) Compatibilidad integral con IPv4/IPv6
b) Equilibrio de carga de servidor avanzado de capa 4/capa 7
   1. HTTP rápido, proxy HTTP completo
   2. Conmutación de Capa 7 de alto rendimiento basada en plantillas con manipulación de encabezado/URL/dominio
   3. Soporte integral de persistencia de aplicaciones de Capa 7
c) Métodos integrales de equilibrio de carga.
d) Round Robin, Least Connections Weighted RR, Weighted LC, Fastest Response, y más
e) aFleX: inspección profunda y transformación de paquetes para personalización, conmutación consciente de la aplicación
f) Monitoreo de salud avanzado
   1. Compatibilidad integral con protocolos: ICMP, TCP, UDP, HTTP, HTTPS, FTP, RTSP, SMTP, POP3, SNMP, DNS, RADIUS, LDAP y más
g) Compatibilidad con comprobación de estado programable de TCL
h) Equilibrio de carga SIP para VoIP
i) Compatibilidad con STARTTLS para correo electrónico seguro (POPS, SMTPS, IMAPS) y LDAPS
j) Compatibilidad con filtro de spam: aplicación de alta velocidad de listas blancas y negras muy grandes
k) Equilibrio de carga del firewall (FWLB)
l) Equilibrio de carga de servidor global (GSLB)
m) Conmutación de caché transparente (TCS)
n) Equilibrio de carga de enlaces (LLB)
o) Equilibrio de carga AAA de diámetro
p) Equilibrio de carga de la base de datos

2) Aceleración de aplicaciones

a) Aceleración y optimización de HTTP
b) Multiplexación de conexión HTTP
c) Almacenamiento en caché HTTP
d) Compresión HTTP

3) Seguridad

a) Firewall de aplicaciones web (WAF)
b) Protección DDoS de próxima generación
   1. Cookies SYN
   2. Detección de anomalías de IP
   3. Prevención de ataques L7
c) Gestión de acceso a aplicaciones (AAM)
d) Cortafuegos de aplicaciones DNS (DAF)
e) Intercepción SSL (SI)
f) Aceleración SSL
   1. Descarga SSL basada en hardware
   2. Compatibilidad con todos los protocolos TCP: terminación SSL, puente SSL (inicio SSL)
   3. Compatibilidad con claves TLS 1.2 y SSL de 4096 bits
g) Reutilización de ID de sesión SSL
h) Limitación de velocidad de conexión/Limitación de conexión

4) Plataforma escalable de alto rendimiento

a) Sistema operativo ACOS
   1. Soporte multinúcleo
   2. Escalado de aplicaciones lineales
   3. Linux en el plano de control
b) ACOS en el plano de datos

5) Networking

a) Capa 2/Capa 3 integrada
b) Modo transparente/modo puerta de enlace
c) Enrutamiento: rutas estáticas, IS-IS (v4/v6), RIPv2/ng, OSPF v2/v3, BGP4+
d) VLAN (802.1Q)
e) Enlace troncal (802.1AX), LACP
f) Listas de control de acceso (ACL)
g) IPv4 tradicional-->IPv4 NAT/NAPT
h) IPv6-->IPv6 NAPT
i) Compatibilidad con Jumbo Frame

6) Migración IPv6/Preservación de IPv4

a) Soporte completo de funciones y administración nativa de IPv6

b) SLB-PT (traducción de protocolo), SLB-64 (IPv4<->IPv6, IPv6<->IPv4)
c) Puertas de enlace a nivel de aplicación (ALG) para FTP, TFTP, RTSP, PPTP, SIP, ICMP, DNS, ESP
d) NAT de nivel de operador (CGNAT), NAT de gran escala (LSN), NAT444, NAT44, NAT46
e) NAT64/DNS64, DS-Lite, 6rd

7) Administración

a) Interfaz de gestión dedicada (Consola, SSH, Telnet, HTTPS)
b) Interfaz gráfica de usuario (GUI) basada en web con localización de idioma
c) Interfaz de línea de comandos estándar de la industria
d) SNMP, Syslog, alertas por correo electrónico
e) Duplicación de puertos
f) API XML de estilo REST (aXAPI)
g) Compatibilidad con LDAP, TACACS+ y RADIUS

En el soporte estará contemplado la escalación de casos con el fabricante y la devolución de mercancía (RMA) en caso presente un algún imprevisto o error que este fuera del soporte local. Como parte de los entregables el proveedor deberá remitir el certificado expedido por la marca para la extensión del soporte y garantía desde 27-08-2024 hasta 31-03-2025. A partir de 01-04-2025 hasta el 31-12-2025 el postor deberá asegurar la disponibilidad del servicio con una solución alterna de la misma marca en modo stand alone con similares funcionalidades técnicas, solamente en el caso fortuito que el A10 Thunder 3030S presente alguna falla de hardware y software que impida su funcionamiento.

h.- **Transferencia de conocimientos**

El postor ganador deberá realizar la transferencia de conocimiento de cada solución al personal del SINFA que administrará la solución según el siguiente detalle:

1) Para la solución Antispam Cisco ESA C195 la transferencia conocimiento de la administración de la solución y sus funcionalidades será considerada para tres (3) personas y ejecutada durante la fecha programada para la actividad N°1 con una duración de ocho (8) horas, por lo que el postor deberá presentar el acta firmada por cada participante como parte de los entregable al término de las actividades.

2) Para la solución Veritas Netbackup 5240 la transferencia conocimiento de la administración de la solución y sus funcionalidades será considerada para tres (3) personas y ejecutada durante la fecha programada para la actividad N°2 con una duración de ocho (8) horas, por lo que el postor deberá presentar el acta firmada por cada participante como parte de los entregable al término de las actividades.

3) Para la solución CheckPoint que incluye el Firewall Checkpoint 5600, Firewall Checkpoint 5900 y CheckPoint Sandblast. TE-1000X, la transferencia conocimiento de la administración de la solución y sus funcionalidades será considerada para cinco (5) personas y ejecutada durante la fecha programada para las actividades N°3, N°4 y N°5 con una duración de ocho (8) horas, por lo que el postor deberá presentar las dos (2) actas firmadas (Firewall y SandBlast) por cada participante como parte de los entregable al término de las actividades.

4) Para la solución Infoblox Trinzic 1405 la transferencia conocimiento de la administración de la solución y sus funcionalidades será considerada para tres (3) personas y ejecutada durante la fecha programada para la actividad N°6 con una duración de ocho (8) horas, por lo que el postor deberá presentar el acta firmada por cada participante como parte de los entregable al término de las actividades.

5) Para la solución A10 Thunder 3030s la transferencia conocimiento de la administración de la solución y sus funcionalidades será considerada para cuatro (4) personas y ejecutada durante la fecha programada para la actividad N° 7 con una duración de ocho (8) horas, por lo que el postor deberá presentar el acta firmada por cada participante como parte de los entregable al término de las actividades.

El postor deberá remitir junto con el informe final las seis (6) actas de transferencia de conocimiento debidamente firmadas por los participantes y membretada por el postor.

2.- PLAN DE TRABAJO

El postor que resulte ganador del Proceso del servicio de Renovación de licencias y la extensión del soporte y garantía, deberá presentar el plan de trabajo previo a la suscripción del contrato:

a.- Presentar su plan de trabajo con su respectivo cronograma de ejecución en función al horario de labores de la institución (lunes a viernes de 08:00 a 16:45); el cual será requisito para el perfeccionamiento del contrato.

b.- El postor deberá presentar en su propuesta la lista del personal que realizarán los trabajos de implementación en el SINFA, las cuales demuestren lo solicitado en el punto h.- REQUISITOS DEL

POSTOR Y PERSONAL TÉCNICO del presente Término de Referencia, mencionada lista contemplará los siguientes datos: nombre completo, apellido paterno, apellido materno y número de DNI o Carné de extranjería para extranjeros, de ser el caso de que algún personal presente impedimentos para realizar el trabajo, deberá ser reemplazado por otro personal con las mismas capacidades técnicas y/o certificaciones requeridas para este proceso previa solicitud formal.

3.- RECURSOS A SER PROVISTOS POR EL PROVEEDOR

a.- **ACREDITACIÓN DE TÉRMINOS DE REFERENCIA DURANTE LA PRESENTACIÓN DE OFERTAS DEL PROCESO:**

1) En el caso de las renovaciones de licencia, el postor deberá presentar en su propuesta técnica los tipos de licencias y la lista de funcionalidades y/o blades de acuerdo con los términos de referencia.

2) El postor deberá presentar una carta del fabricante donde refleje ser partner autorizado y haga referencia al proceso indicado, la cual podrá ser entregada a la firma del contrato.

b.- **IMPLEMENTACIÓN**

1) La instalación y configuración se realizará en coordinación con el Dpto. Arquitectura Digital del SINFA, posterior a la entrega de los certificados de las licencias y soporte indicados anteriormente en el párrafo 6.-,

2) La implementación incluye las siguientes etapas:
   a) Instalación de las licencias según corresponda.
   b) Verificación de la vigencia de las extensiones de suscripción de las soluciones en las consolas de gestión del mismo equipo (webui, cli), y/o consola de gestión central y/o portal del fabricante junto con el personal de la Entidad.
   c) Configuración de políticas, exclusiones y ejecución de tareas junto con el personal de la Entidad al término de la implementación de las extensiones según corresponda.

3) El Postor contemplará el (los) softwares de conexión remota que sea(n) necesario(s) para la correcta implementación de las licencias de las soluciones ofertadas, tales como: MobaExtern, Webex, Putty, etc.

c.- **ENTREGA, INSTALACIÓN, CONFIGURACIÓN Y TRANSFERENCIA DE CONOCIMIENTO**

La entrega, instalación, configuración y transferencia de conocimiento de la renovación de licencias y extensión de soporte y garantía de las soluciones; se realizará en el Cuartel General de la FAP – Dpto. de Arquitectura Digital del SINFA en un plazo de sesenta y cinco (65) días, el mismo que se realizará durante la ejecución contractual y deberá establecerse en el Plan de Trabajo de acuerdo con las fechas indicadas.

d.- **PERIODO DE RENOVACIÓN DE LICENCIAS (LICENCIAMIENTO)**

El periodo de licenciamiento será de acuerdo al siguiente detalle:

N°	FABRICANTE	REQUERIMIENTO
1	CHECKPOINT	EXTENSION DE SUSCRIPCION DE LICENCIAS DEL FIREWALL 5600 PERIODO (28 NOV 2024 – 31 DIC 2025)
2		EXTENSION DE SUSCRIPCION DE LICENCIAS Y DEL FIREWALL 5900 PERIODO (28 NOV 2024 – 31 DIC 2025)
3		EXTENSION DE SUSCRIPCION DE LICENCIAS DEL SANDBLAST TE - 1000X PERIODO (28 NOV 2024 – 31 DIC 2025)
4	CISCO	EXTENSION DE SUSCRIPCION DE LICENCIAS PARA 500 BUZONES DEL ANTISPAM ESA C195 PERIODO (12 JUL 2024 – 31 DIC 2025)

e.- **PERIODO DE EXTENSIÓN DE SOPORTE Y GARANTIA**

El periodo de extensión de soporte y garantía del fabricante será de acuerdo al siguiente detalle:

N°	FABRICANTE	REQUERIMIENTO
1	CHECKPOINT	SOPORTE FABRICA HW Y SW DEL FIREWALL 5600 PERIODO (28 NOV 2024 – 31 DIC 2025)
2		SOPORTE FABRICA HW Y SW DEL FIREWALL 5900 PERIODO (28 NOV 2024 – 31 DIC 2025)
3		SOPORTE FABRICA HW Y SW DEL SANDBLAST TE - 1000X PERIODO (28 NOV 2024 – 31 DIC 2025)
4	INFOBLOX	EXTENSION DE SOPORTE FABRICA HW Y SW DEL DNS, DHCP, IPAM TRINZIC 1415 PERIODO (08 NOV 2024 – 31 DIC 2025)

5	A10 NETWORKS **(*)**	EXTENSION DE SOPORTE FABRICA HW Y SW DEL BALANCEADOR / SSL THUNDER 3030S PERIODO (27 AGO 2024 – 31 MAR 2025)
6	VERITAS **(*)**	EXTENSION DE SOPORTE FABRICA HW Y SW DE LA SOLUCION DE RESPALDO Y RESTAURACION PERIODO (22 JUL 2024 – 31 OCT 2025)

NOTA (*):
Para el caso de las soluciones de A10 Thunder 3030S y el Veritas NetBackup 5240, el postor ganador deberá brindar apoyo técnico respecto a optimización de políticas y configuración con su personal certificado hasta el 31 de diciembre del 2025. Solamente en el caso fortuito que el A10 Thunder 3030S y/o el Veritas NetBackup 5240 presenten alguna falla de hardware y/o software que impida su funcionamiento, el postor deberá asegurar la disponibilidad con una solución alterna de la misma marca con similares funcionalidades técnicas que tenga soporte y garantía vigente.

f.- **REFERIDOS AL SOPORTE TÉCNICO**

1) El soporte técnico se efectuará a través de la línea telefónica, correo electrónico o en sitio cuando se requiera. El soporte ante cualquier incidencia se aplica de la siguiente modalidad 24 x 7 x 365 y será realizado por personal especialista certificado por el fabricante del producto ofertado.

2) El postor debe brindar un número y correo de su Centro de Atención de Incidentes, soporte y/o atención, para el reporte de incidencias. Al ocurrir un "incidente", el personal técnico de la Institución reportará por correo electrónico o vía telefónica al Centro de Atención del Postor, quien registrará el requerimiento y proporcionará un número de ticket para realizar el seguimiento respectivo. Para garantizar en toda circunstancia la posibilidad de escalamiento del servicio del fabricante para una oportuna solución de los eventos presentados.

3) El postor realizará las actualizaciones de firmware y software recomendadas por el fabricante de cada solución dentro del periodo de licenciamiento o suscripción contratado por equipamiento, así como verificar que dicho proceso de actualización no comprometa la disponibilidad de los servicios.

4) El postor deberá garantizar el adecuado funcionamiento de los equipos por el periodo contratado asumiendo el tiempo de end of life de la marca hasta la finalización mencionada en estos términos de referencia. En caso el tiempo de soporte y garantía de las marcas de cada solución sea menor a la garantía comercial (A10 Thunder 3030S y Veritas NetBackup 5240), el postor ganador, de ser necesario, deberá brindar apoyo técnico respecto a optimización de políticas y configuración con su personal certificado por cada una de las marcas hasta el término de la garantía comercial (31-12-2025). En el caso que el problema de mencionadas marcas (A10 y Veritas) fuera una falla fortuita de hardware y/o software, el postor deberá reemplazar en calidad de servicio mencionado equipamiento con una solución de la misma marca que tenga soporte vigente hasta el 31-12-2025.

g.- **GARANTÍA COMERCIAL**

El periodo de garantía de todas las soluciones que forman parte del servicio será hasta el 31-12-2025.

h.- **REQUISITOS DEL POSTOR Y PERSONAL TÉCNICO**

1) **Del POSTOR**
El POSTOR deberá ser partner autorizado de cada una de las marcas ofertadas, se deberá acreditar mediante la presentación de una carta del fabricante haciendo referencia al proceso, la cual podrá ser entregada a la firma del contrato.

2) **DEL PERSONAL TÉCNICO**
El POSTOR deberá contar con el personal técnico para el cumplimiento de los siguientes cargos de acuerdo a lo siguiente:

a) **UN (01) JEFE DE PROYECTO**

Años de Experiencia y conocimientos:
Experiencia en gestionar proyectos de soluciones de seguridad informática o ciberseguridad (mínima de 3 años y con una antigüedad en esos trabajos máxima de 6 años).

Carrera Profesional:
1) Ingeniería Electrónica, Sistemas, Industrial, Computación y Sistemas o Comunicaciones, Ingeniería de telecomunicaciones, Ingeniería Informática y de Sistemas.
2) Grado Académico: Titulado (deberá figurar en el sistema de la SUNEDU con la finalidad de verificar la veracidad del grado académico, de no estar registrado será causal de descalificación)
3) Debe estar capacitado y contar con certificación vigente en PMP (Project Management Professional).

Para tal efecto el postor deberá acreditar estos requisitos con la presentación de copia simple del Título Profesional correspondiente. La experiencia del personal se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y sus respectivas conformidades que de manera fehaciente demuestre la experiencia del personal propuesto.

b) **ESPECIALISTAS EN LAS SOLUCIONES DEL SERVICIO**
Mínimo 01 especialista con certificado vigente por cada solución del servicio detallado en el párrafo 6.-.

Años de Experiencia y conocimientos:
Experiencia en instalación y/o implementación de herramientas o soluciones de seguridad informática o ciberseguridad (mínima de 2 años con una antigüedad en esos trabajos máxima de 5 años), en las marcas de los servicios contratados, la cual deberá ser presentada en la propuesta con una copia simple de las certificaciones.

Carrera Profesional:
1. Ingeniería de Sistemas, Electrónica, Redes y Comunicaciones, Computación e Informática, computación y sistemas, o Telecomunicaciones o profesional técnico titulado de la carrera de Redes y Comunicaciones, Computación e Informática o Telecomunicaciones o Soporte y Mantenimiento de Equipos de Computación.
2. Certificado técnico vigente en cada una de las soluciones ofertadas.

La experiencia del personal técnico se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y sus respectivas conformidades o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación oficial que de manera fehaciente demuestre la experiencia del personal propuesto.

4.- RECURSOS A SER PROVISTOS POR LA ENTIDAD

a.- La entidad brindará los recursos de hardware necesarios para la implementación de las extensiones de licencia según corresponda.

b.- La ENTIDAD proporcionará los pases para el ingreso del personal a los lugares donde se realizará el servicio.

5.- REGLAMENTOS TÉCNICOS, NORMAS METROLÓGICAS Y/O SANITARIAS NACIONALES

a.- Deberán de cumplir con las Normas técnicas vigentes.

6.- NORMAS TÉCNICAS
Todos los trabajos inherentes al servicio prestado, deberán estar de acuerdo a las Normas técnicas vigentes.

7.- SEGUROS
El Postor debe cumplir con las regulaciones laborales respecto a la seguridad de su personal, que debe contar con las pólizas de seguro para trabajos de alto riesgo (Seguro Complementario de Trabajo de Riesgo – SCTR) emitida por empresas aseguradoras autorizadas por la SBS. Asimismo, dichos seguros deben encontrarse vigentes durante toda la prestación del presente servicio y deberá ser acreditado al inicio efectivo del servicio.

El Postor debe garantizar que su personal cuente con las herramientas, indumentaria y mecanismos de seguridad adecuados. El Postor es responsable de los daños y/o accidentes ocasionados a terceros, durante la ejecución de las actividades del servicio.

Todo este trabajo encomendado se realizará con los seguros correspondientes (SCTR vigentes e implementos EPP), bajo responsabilidad del Postor de velar por su personal técnico. No se permitirá que el personal técnico realice labores sin contar con los seguros respectivos y los mecanismos de seguridad y protección.

El Postor se compromete a cumplir y respetar cada una de las medidas de seguridad previstas en el protocolo de la entidad (SINFA).

8.- GARANTÍA TÉCNICA Y/O COMERCIAL
Estará vigente para todas las soluciones que forman parte del servicio: hasta el 31-12-2025.

Ante la presentación de algún problema que genere la inoperatividad de cualquiera de las soluciones del producto ofertado durante el periodo que demande el servicio, El POSTOR deberá al término de la distancia, en un plazo máximo de 3 horas, previa coordinación con el encargado deberá apersonarse a brindar solución, con la finalidad que los servicios de cada solución no sean afectados.

9.- VISITA
Durante la convocatoria, el participante podrá realizar una visita de campo en el lugar donde se prestará el servicio objeto de la convocatoria, de tal manera que pueda tener la información suficiente para la presentación de su oferta técnica y económica. Asimismo, de no realizar la citada visita, posteriormente no podrá argumentar desconocimiento y/o falta de información de los alcances del servicio, asumiendo los costos necesarios para su correcta ejecución y funcionamiento. Dichas visitas podrán realizarse de lunes a viernes (laborables) en el horario desde las 8:00 a 12:30 horas y desde las 13:30 a 16:30 horas previa coordinación a través del correo sinfa_tic@fap.mil.pe.

10.- LUGAR Y PLAZO DE EJECUCIÓN DEL SERVICIO
La prestación se realizará en la ciudad de Lima, en las Instalaciones del Servicio de Informática en el Cuartel General de la FAP, sito en Av., La Peruanidad SN – Jesús María. El plazo de duración del servicio será según cuadro de cronograma de actividades

Actividades	Plazo
Se realizarán siete (7) actividades previas a la presentación del informe final por parte del postor	**El plazo para la realización de las siete (7) actividades será de sesenta (65) días calendarios de acuerdo con el siguiente detalle:**
Actividad N° 1: Extensión de Suscripción de Licencias para 500 Buzones del Antispam Cisco ESA C195 y soporte de fábrica de hardware y software.	Del 9 hasta el 21 de julio del 2024 para la ejecución de la actividad y la transferencia de conocimientos de ocho (8) horas para la presente solución.
Actividad N° 2: Extensión de soporte fábrica de Hardware y Software de la solución de respaldo y restauración Veritas Netbackup 5240	Del 22 de julio hasta el 1 de agosto del 2024 para la ejecución de la actividad y la transferencia de conocimientos de ocho (8) horas para la presente solución.
Actividad N° 3: Extensión de Suscripción de Licencias, soporte de fábrica de hardware y software del Firewall CheckPoint 5600 **Actividad N° 4:** Extensión de Suscripción de Licencias, soporte de fábrica de hardware y software del Firewall CheckPoint 5900. **Actividad N° 5**: Extensión de Suscripción de Licencias, soporte de fábrica de hardware y software del CheckPoint Sandblast. TE-1000X	Del 2 hasta el 16 de agosto del 2024 para la ejecución de la actividad y la transferencia de conocimientos de ocho (8) horas para las presentes soluciones.
Actividad N° 6: Extensión de soporte y garantía de fábrica Hardware y Software del DNS, DHCP, IPAM Infoblox Trinzic 1405	Del 17 hasta el 26 de agosto del 2024 para la ejecución de la actividad y la transferencia de conocimientos de ocho (8) horas para la presente solución.
Actividad N° 7: Extensión de soporte y garantía de fabrica Hardware y Software del balanceador de carga/SSL A10 Thunder 3030s, y presentación del informe final	Del 27 de agosto hasta el 11 de setiembre del 2024 para la ejecución de la actividad y la transferencia de conocimientos de ocho (8) horas para la presente solución, y presentación del informe final

11.- ADELANTOS
La entidad no ha previsto adelantos para la ejecución de este servicio.

12.- CONFIDENCIALIDAD
Por ser una base militar el postor ganador deberá contar preferentemente con personal de nacionalidad peruana, con toda su documentación en regla para ser registrados en la Oficina de Seguridad Militar del SINFA. Así mismo, el postor deberá entregar la relación de trabajadores como documentación oficial para la suscripción del contrato.

13.- CONFORMIDAD DEL SERVICIO
La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por el jefe del Departamento de Arquitectura Digital en el plazo máximo de siete (7) días posterior a la entrega del informe final por parte del postor ganador.

De existir observaciones, LA ENTIDAD las comunicará al POSTOR, 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 POSTOR no cumpliese a cabalidad con la subsanación, LA ENTIDAD puede otorgar al POSTOR periodos adicionales para las correcciones pertinentes. En este supuesto

corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar.

14.- FORMA DE PAGO
De acuerdo con el artículo 171° del Reglamento, para efectos del pago de las contraprestaciones ejecutadas por el Postor, la Entidad deberá contar con la siguiente documentación:

a.- Informe técnico especializado del representante de la Empresa ganadora. (donde incluirá fotos de las actividades realizadas antes, durante y después), incluidas las actas de transferencia de conocimientos**.**

b.- Informe del funcionario responsable del área usuaria (jefe del Departamento de Arquitectura Digital), emitiendo la conformidad de la prestación efectuada.

c.- Acta de Recepción y Conformidad debidamente firmada por el jefe del área usuaria, jefe del departamento de Abastecimiento y Comando del Servicio de Informatica

Factura.
Pago único a través de CCI.
EL PAGO SE REALIZARÁ A TRAVES DE TRANSFERENCIA BANCARIA.

15.- OTRAS PENALIDADES

N°	SUPUESTO DE APLIACIÓN DE PENALIDAD	FORMULA DE CÁLCULO	PROCEDIMIENTO
1	Tener trabajador menor de 18 años	3 UIT Por día y/o evento	Mediante informe técnico del inspector o supervisor del servicio
2	Paralización de labores por causas imputables al Postor	1 UIT Por día y/o evento	
3	Paralizaciones de labores que puedan realizar su personal por incumplimiento en pagos y beneficios sociales.	1 UIT Por día y/o evento	
4	Cuando el Postor no cumpla con controlar o dotar a su personal con el uso de los implementos de seguridad.	1 UIT Por día y/o evento	
5	Cuando los profesionales y/o técnicos no se encuentren en el servicio conforme el cronograma de trabajo establecido.	1 UIT Por día y/o evento	
6	Cuando los profesionales y/o técnicos no cumplan y/o utilicen procedimientos que contravengan las normas técnicas y de calidad	3 UIT Por día y/o evento	

16.- RESPONSABILIDAD DEL CONTRATISTA

a.- Crear, actualizar o suministrar toda documentación a la entidad, relacionados al servicio.

b.- En caso de acceso a una plataforma de base de conocimientos, deberá entregar un acceso a través del correo electrónico: sinfa_tic@fap.mil.pe**.**

c.- Para el caso que el POSTOR tuviera que destacar personal para instalación y mantenimiento de los componentes, deberá proporcionar mobiliario, máquinas y todo elemento necesario para correcta implementación, quedando como única responsabilidad de la entidad, brindar el espacio físico necesario, puntos de red y energía eléctrica.

d.- El POSTOR se compromete a cumplir y observar lo establecido en la Ley de Seguridad y Salud en el Trabajo (aprobado mediante ley N° 29783) y en su reglamento (aprobado mediante Decreto Supremo N° 005-2012-TR). durante la ejecución de las prestaciones de servicios a su cargo. obligándose a implementar, dotar, proveer y/o suministrar a cada uno de sus trabajadores los implementos de seguridad que corresponda de acuerdo al grado y/o nivel de riesgo que pueda evidenciarse en el desarrollo de las actividades propias de la presente adquisición, dentro de las instalaciones de la Entidad. así como garantizar la contratación de los respectivos seguros de acuerdo a la normatividad vigente.

e.- Del mismo modo el POSTOR se compromete a cumplir y respetar cada una de las medidas de seguridad de la Entidad.

3.2. REQUISITOS DE CALIFICACIÓN

B.3	**CALIFICACIONES DEL PERSONAL CLAVE**
B.3.1	**FORMACIÓN ACADÉMICA**
	Requisitos: **01 Jefe de Proyecto:** Titulado en Ingeniería electrónica y/o de sistemas y/o Industrial y/o Computación y/o informático y/o Ingeniero de Comunicaciones y/o telecomunicaciones. **01 Especialista en Soluciones del Servicio:** Titulado en Ingeniería de Sistemas, Electrónica, Redes y Comunicaciones, Computación e Informática, computación y sistemas, o Telecomunicaciones o profesional técnico titulado de la carrera de Redes y Comunicaciones, Computación e Informática o Telecomunicaciones o Soporte y Mantenimiento de Equipos de Computación Acreditación: El grado y título será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: *https://titulosinstitutos.minedu.gob.pe/*, según corresponda. **Importante para la Entidad** *El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.* En caso que no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
B.3.2	**CAPACITACIÓN**
	Requisitos: Curso de capacitación en PMP (Project Management Professional del personal clave requerido como **Jefe de Proyecto.** **Especialista en Soluciones del Servicio**: Deberá presentar sus Certificaciones por cada solución del servicio detallado en los términos de referencia. Acreditación: Se acreditará con copia simple de la certificación vigente. **Importante** *Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas lectivas, según la normativa de la materia.*

B.4	**EXPERIENCIA DEL PERSONAL CLAVE**

Requisitos:

Jefe de Proyecto:
Experiencia en gestionar proyectos de soluciones de seguridad informática o ciberseguridad (mínima de 3 años y con una antigüedad en esos trabajos máxima de 6 años).

Especialista en Soluciones del Servicio:
Experiencia en instalación y/o implementación de herramientas o soluciones de seguridad informática o ciberseguridad (mínima de 2 años con una antigüedad en esos trabajos máxima de 5 años), en las marcas de los servicios contratados, la cual deberá ser presentada en la propuesta.

De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

Acreditación:

La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.

Importante

- *Los docum**entos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.***
- *En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.*
- *Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.*
- *Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.*

C	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a tres millones trescientos mil soles (S/. 3´300,000.00), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se consideran servicios similares a los siguientes: Venta y/o Servicios de renovación de licencias, venta y/o servicio de garantía extendida de equipos de ciberseguridad que cumplan las funciones de Firewall, balanceador de carga, antispam, backup, dns/dhcp. Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago[11], correspondientes a un máximo de veinte (20) contrataciones. En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad. En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados. En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato. Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales. Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9.** Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda. Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad.

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

> *"… el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"*
> *(…)*
> *"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".*

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

Importante

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

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

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

CAPÍTULO IV
FACTORES DE EVALUACIÓN

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

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

FACTOR DE EVALUACIÓN	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
A. PRECIO	
Evaluación: Se evaluará considerando el precio ofertado por el postor. Acreditación: Se acreditará mediante el documento que contiene el precio de la oferta **(Anexo N° 6)**.	La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $$Pi = \frac{Om \times PMP}{Oi}$$ **i** = Oferta **Pi** = Puntaje de la oferta a evaluar **Oi** = Precio i **Om** = Precio de la oferta más baja **PMP** = Puntaje máximo del precio 90 **puntos**

H. MEJORAS A LOS TÉRMINOS DE REFERENCIA	
Evaluación: Servicio de Análisis de Vulnerabilidades a 10 activos del Centro de Datos Institucional en un escenario de pruebas Internas. I. MARCO METODOLOGICO El marco metodológico de la evaluación se deberá basar en: PTES Penetration Testing Execution Standard, que es un estándar desarrollado por expertos en el rubro de la seguridad informática para realizar una evaluación que contemple el proceso de revisión de seguridad con un objetivo principal, encontrar aquellas vulnerabilidades existentes, y aquellas brechas de seguridad que pudieran facilitar a un atacante tomar control total o parcial de la organización. NIST SP 800-115, que es una guía técnica para las evaluaciones y pruebas de seguridad de la información, orientada a la comprobación de aspectos técnicos en sistemas informáticos o redes de datos. OSSTMM Open Source Security Testing Methodology Manual, que es una metodología de código abierto utilizada por expertos en seguridad para realizar trabajos de Ethical Hacking. Esta metodología es un marco referente en el mercado e incluso biografía obligatoria en varios libros y papers de seguridad. I. DESCRIPCIÓN DE PRUEBAS Las actividades por desarrollar son: Pruebas Internas Se deberá hacer un escaneo de la red detectando las posibles vulnerabilidades sobre los activos tecnológicos. El trabajo deberá realizarse 4 veces en un periodo de 12 meses.	**10 puntos**

I. ENTREGABLES Informe Técnico a) Alcance de las pruebas b) Marco metodológico c) Resumen de vulnerabilidades d) Nombre de la vulnerabilidad e) Tipo de vulnerabilidad f) Nivel de impacto g) Descripción de los hallazgos h) Entorno de afectación i) Remediación (recomendación técnica) La información obtenida en el proceso de análisis deberá ser eliminada a través de un proceso de BORRADO SEGURO de las computadoras de los consultores a cargo del trabajo de campo. Acreditación: Se acreditará únicamente mediante la presentación de una DECLARACIÓN JURADA, la misma que deberá indicar en su contenido: El uso del marco metodológico solicitado, descripción de las pruebas solicitadas y los entregables solicitados. **Importante** • *De conformidad con la Opinión N° 144-2016-OSCE/DTN, constituye una mejora, todo aquello que agregue un valor adicional al parámetro mínimo establecido en las especificaciones técnicas o términos de referencia, según corresponda, mejorando su calidad o las condiciones de su entrega o prestación, sin generar un costo adicional a la Entidad.* • *En este factor se pueden incluir aspectos referidos a la sostenibilidad ambiental o social, tales como el compromiso de que durante la ejecución del contrato se verifiquen condiciones de igualdad de género o de inclusión laboral de personas con discapacidad; el uso de equipos energéticamente eficientes o con bajo nivel de ruido, radiaciones, vibraciones, emisiones, etcétera; la implementación de medidas de ecoeficiencia; el uso de insumos que tengan sustancias con menor impacto ambiental; la utilización de productos forestales de fuentes certificadas, orgánicos o reciclados, el manejo adecuado de residuos sólidos, entre otros.*	
PUNTAJE TOTAL	**100 puntos**

Importante

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

CAPÍTULO V
PROFORMA DEL CONTRATO

Importante

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

Conste por el presente documento, la contratación del **SERVICIO DE RENOVACIÓN DE LICENCIAS, EXTENSIÓN DE SOPORTE Y GARANTÍA DE LOS EQUIPOS DE TECNOLOGÍA DE LA INFORMACIÓN DEL CENTRO DE DATOS SINFA**], que celebra de una parte la Fuerza Aérea del Perú, en adelante LA ENTIDAD, con RUC Nº 20144364059, con domicilio legal en [……], representada por [……..…], identificado con DNI Nº [……], y de otra parte […….....], con RUC Nº [.....], con domicilio legal en […….....], inscrita en la Ficha N° […….....] Asiento N° […….....] del Registro de Personas Jurídicas de la ciudad de [……], debidamente representado por su Representante Legal, […….....], con DNI N° [……..], según poder inscrito en la Ficha N° [……..], Asiento N° [……] del Registro de Personas Jurídicas de la ciudad de [……], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [……..], el comité de selección adjudicó la buena pro del **CONCURSO PÚBLICO Nº** 005-2024-FAP-SINFA para la contratación de **SERVICIO DE RENOVACIÓN DE LICENCIAS, EXTENSIÓN DE SOPORTE Y GARANTÍA DE LOS EQUIPOS DE TECNOLOGÍA DE LA INFORMACIÓN DEL CENTRO DE DATOS SINFA**, 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 contratación del **SERVICIO DE RENOVACIÓN DE LICENCIAS, EXTENSIÓN DE SOPORTE Y GARANTÍA DE LOS EQUIPOS DE TECNOLOGÍA DE LA INFORMACIÓN DEL CENTRO DE DATOS SINFA**

CLÁUSULA TERCERA: MONTO CONTRACTUAL

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

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

CLÁUSULA CUARTA: DEL PAGO[12]

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 Regla
mento 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.

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

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

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

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de 65 DÍAS CALENDARIOS, el mismo que se computa desde (DESDE LA FECHA QUE SE ESTABLEZCA EN EL CONTRATO O DESDE LA FECHA EN QUE SE CUMPLAN LAS CONDICIONES PREVISTAS EN EL CONTRATO PARA EL INICIO DE LA EJECUCIÓN, DEBIENDO INDICAR LAS MISMAS EN ESTE ULTIMO CASO].

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

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

CLÁUSULA SÉTIMA: GARANTÍAS

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

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

Importante
Al amparo de lo dispuesto en el numeral 149.4 del artículo 149 del Reglamento de la Ley de Contrataciones del Estado, en el caso de contratos periódicos de prestación de servicios en general, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato original como garantía de fiel cumplimiento de contrato, debe consignarse lo siguiente: *"De fiel cumplimiento del contrato:* [CONSIGNAR EL MONTO]*, a través de la retención que debe efectuar LA ENTIDAD, durante la primera mitad del número total de pagos a realizarse, de forma prorrateada, con cargo a ser devuelto a la finalización del mismo."*

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

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

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

CLÁUSULA DÉCIMA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 168 del Reglamento de la Ley de Contrataciones del Estado. La conformidad será otorgada por El Departamento de Arquitectura digital en el plazo máximo de [CONSIGNAR SIETE (7) DÍAS O MÁXIMO QUINCE (15) DÍAS, EN CASO SE REQUIERA EFECTUAR PRUEBAS QUE PERMITAN VERIFICAR EL CUMPLIMIENTO DE LA OBLIGACIÓN] días de producida la recepción.

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

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

CLÁUSULA UNDÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

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

CLÁUSULA DUODÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

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

El plazo máximo de responsabilidad del contratista es de un año contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA TERCERA: PENALIDADES

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

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

Donde:

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

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

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

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

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

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

CLÁUSULA DÉCIMA CUARTA: RESOLUCIÓN DEL CONTRATO

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

CLÁUSULA DÉCIMA QUINTA: RESPONSABILIDAD DE LAS PARTES

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

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

CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN

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

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

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

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

CLÁUSULA DÉCIMA SÉTIMA: MARCO LEGAL DEL CONTRATO

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

CLÁUSULA DÉCIMA OCTAVA: SOLUCIÓN DE CONTROVERSIAS[13]

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

13 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).

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

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

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

CLÁUSULA DÉCIMA NOVENA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

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

CLÁUSULA VIGÉSIMA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

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

DOMICILIO DE LA ENTIDAD: Av. La Peruanidad S/N Jesús María.

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

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

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

"LA ENTIDAD"	"EL CONTRATISTA"

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley Nº 27269, Ley de Firmas y Certificados Digitales[14].

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

ANEXOS

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 005-2024-FAP-SINFA
Presente.-

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

Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[15]		Sí		No	
Correo electrónico :					

Autorización de notificación por correo electrónico:

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios16

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.

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

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

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

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 005-2024-FAP-SINFA
Presente.-

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

Datos del consorciado 1					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[17]		Sí		No	
Correo electrónico :					

Datos del consorciado 2					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[18]		Sí		No	
Correo electrónico :					

Datos del consorciado …					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[19]		Sí		No	
Correo electrónico :					

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

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

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

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

18 Ibídem.

19 Ibídem.

4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios20

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

[CONSIGNAR CIUDAD Y FECHA]

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

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

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

ANEXO Nº 2

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 005-2024-FAP-SINFA
Presente.-

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

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

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

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

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

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

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

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

ANEXO Nº 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 005-2024-FAP-SINFA
Presente.-

Es grato dirigirme a usted, para hacer de su conocimiento que luego de haber examinado las bases y demás documentos del procedimiento de la referencia y, conociendo todos los alcances y las condiciones detalladas en dichos documentos, el postor que suscribe ofrece el servicio de **SERVICIO DE RENOVACIÓN DE LICENCIAS, EXTENSIÓN DE SOPORTE Y GARANTÍA DE LOS EQUIPOS DE TECNOLOGÍA DE LA INFORMACIÓN DEL CENTRO DE DATOS SINFA,** de conformidad con los Términos de Referencia que se indican en el numeral 3.1 del Capítulo III de la sección específica de las bases y los documentos del procedimiento.

[CONSIGNAR CIUDAD Y FECHA]

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

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

ANEXO Nº 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 005-2024-FAP-SINFA
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO Nº 5

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 005-2024-FAP-SINFA
Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta al **CONCURSO PÚBLICO Nº 005-2024-FAP-SINFA**

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]	[%] 21
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]	
2.	OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2]	[%] 22
	[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]	
	TOTAL OBLIGACIONES	100%23

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

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

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

[CONSIGNAR CIUDAD Y FECHA]

.....	.....
Consorciado 1	**Consorciado 2**
Nombres, apellidos y firma del Consorciado 1	**Nombres, apellidos y firma del Consorciado 2**
o de su Representante Legal	**o de su Representante Legal**
Tipo y N° de Documento de Identidad	**Tipo y N° de Documento de Identidad**

Importante

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

ANEXO Nº 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 005-2024-FAP-SINFA
Presente.-

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

CONCEPTO	PRECIO TOTAL
TOTAL	

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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

Importante para la Entidad

- *En caso de procedimientos según relación de ítems, consignar lo siguiente:*
  "El postor puede presentar el precio de su oferta en un solo documento o documentos independientes, en los ítems que se presente".
- *En caso de contrataciones que conllevan la ejecución de prestaciones accesorias, consignar lo siguiente:*
  "El postor debe detallar en el precio de su oferta, el monto correspondiente a la prestación principal y las prestaciones accesorias".

Incluir o eliminar, según corresponda

ANEXO Nº 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 005-2024-FAP-SINFA
Presente.-

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

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP 24	FECHA DE LA CONFORMIDAD DE SER EL CASO25	EXPERIENCIA PROVENIENTE26 DE:	MONEDA	IMPORTE27	TIPO DE CAMBIO VENTA[28]	MONTO FACTURADO ACUMULADO 29
1										
2										

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

25 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.

26 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"*.

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

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

29 Consignar en la moneda establecida en las bases.

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP 24	FECHA DE LA CONFORMIDAD DE SER EL CASO25	EXPERIENCIA PROVENIENTE26 DE:	MONEDA	IMPORTE27	TIPO DE CAMBIO VENTA[28]	MONTO FACTURADO ACUMULADO 29
3										
4										
5										
6										
7										
8										
9										
10										
	…									
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO Nº 9

DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 005-2024-FAP-SINFA
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

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

ANEXO N° 12

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

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº 005-2024-FAP-SINFA
Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

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