BASES ESTÁNDAR DE ADJUDICACIÓN SIMPLIFICADA 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 órgano encargado de las contrataciones o comité de selección, según corresponda y por los proveedores.
4	*Advertencia* • *Abc*	Se refiere a advertencias a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda y por los proveedores.
5	Importante para la Entidad • Xyz	Se refiere a consideraciones importantes a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda y deben ser eliminadas una vez culminado 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	Automática: 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 los 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 marzo, junio y diciembre de 2019 y en julio 2020

MARINA DE GUERRA DEL PERU
DIRECCIÓN DE TELEMÁTICA DE LA MARINA

BASES ESTÁNDAR DE ADJUDICACIÓN SIMPLIFICADA PARA LA CONTRATACIÓN DE SERVICIOS EN GENERAL

ADJUDICACIÓN SIMPLIFICADA N° 020-2021 MGP/DIRTEL DERIVADO DEL CONCURSO PÚBLICO CP N° 004-2021

CONTRATACIÓN DEL "SERVICIO DE RENOVACIÓN DE LICENCIAMIENTO DE SOFTWARE DE LA PLATAFORMA DE SERGURIDAD/SERVICIO PP-0135"

PAC N° 113

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)

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

CAPÍTULO I
ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

La formulación de consultas y observaciones a las bases se efectúa de conformidad con lo establecido en los numerales 72.1 y 72.2 del artículo 72 del Reglamento, así como el literal a) del artículo 89 del Reglamento.

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

La absolución de consultas, observaciones e integración de las bases se realizan conforme a las disposiciones previstas en el numeral 72.4 del artículo 72 del Reglamento y el literal a) del artículo 89 del Reglamento.

Importante

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

1.6. FORMA DE PRESENTACIÓN DE OFERTAS

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

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

Importante

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

1.7. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

Importante

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

En la apertura electrónica de la oferta, el órgano encargado de las contrataciones o el comité de selección, según corresponda, verifica la presentación de lo exigido en la sección específica de las bases de conformidad con el numeral 73.2 del artículo 73 del Reglamento y determina si las ofertas responden a las características y/o requisitos 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.

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

1.8. EVALUACIÓN DE LAS OFERTAS

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

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

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

Importante

En el caso de contratación de servicios en general que se presten fuera de la provincia de Lima y Callao, cuyo valor estimado no supere los doscientos mil Soles (S/ 200,000.00), a solicitud del postor se asigna una bonificación equivalente al diez por ciento (10%) sobre el puntaje total obtenido por los postores con domicilio en la provincia donde prestará el servicio, o en las provincias colindantes, sean o no pertenecientes al mismo departamento o región. El domicilio es el consignado en la constancia de inscripción ante el RNP[1]. Lo mismo aplica en el caso de procedimientos de selección por relación de ítems, cuando algún ítem no supera el monto señalado anteriormente.

1.9. CALIFICACIÓN DE OFERTAS

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

1.10. SUBSANACIÓN DE LAS OFERTAS

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

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

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

1.11. RECHAZO DE LAS OFERTAS

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

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

[1] La constancia de inscripción electrónica se visualizará en el portal web del Registro Nacional de Proveedores: www.rnp.gob.pe

1.12. OTORGAMIENTO DE LA BUENA PRO

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

1.13. CONSENTIMIENTO DE LA BUENA PRO

Cuando se hayan presentado dos (2) o más ofertas, el consentimiento de la buena pro se produce a los cinco (5) días hábiles siguientes de la notificación de su otorgamiento, sin que los postores hayan ejercido el derecho de interponer el recurso de apelación.

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

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

Importante

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

CAPÍTULO II
SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

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

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

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

Importante

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

  Luego de otorgada la buena pro no se da a conocer las ofertas cuyos requisitos de calificación no fueron analizados y revisados por el órgano encargado de las contrataciones o el comité de selección, según corresponda.

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

- *El recurso de apelación se presenta ante la Mesa de Partes del Tribunal o ante las oficinas desconcentradas del OSCE, o en la Unidad de Trámite Documentario de la Entidad, según corresponda.*

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

La apelación contra el otorgamiento de la buena pro o contra los actos dictados con anterioridad a ella se interpone dentro de los cinco (5) días hábiles siguientes de haberse notificado el otorgamiento de la buena pro.

La apelación contra los actos dictados con posterioridad al otorgamiento de la buena pro, contra la declaración de nulidad, cancelación y declaratoria de desierto del procedimiento, se interpone dentro de los cinco (5) días hábiles siguientes de haberse tomado conocimiento del acto que se desea impugnar.

CAPÍTULO III
DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

El contrato se perfecciona con la suscripción del documento que lo contiene, salvo en los contratos cuyo monto del valor estimado no supere los cien mil Soles (S/ 100,000.00), en los que se puede perfeccionar con la recepción de la orden de servicios, conforme a lo previsto en la sección específica de las bases.

En el caso de procedimientos de selección por relación de ítems, se puede perfeccionar el contrato con la suscripción del documento o con la recepción de una orden de servicios, cuando el valor estimado del ítem corresponda al parámetro establecido en el párrafo anterior.

Importante

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

Importante

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 original, 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.

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

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 cuyos montos sean iguales o menores a cien mil Soles (S/ 100,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias. Dicha excepción también aplica a los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados no superen el monto señalado anteriormente, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

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

Importante

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

Advertencia

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

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

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

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

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

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

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

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

CAPÍTULO I
GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre	:	MARINA DE GUERRA DEL PERÚ – DIRECCIÓN DE TELEMÁTICA DE LA MARINA
RUC N°	:	20153408191
Domicilio legal	:	Av. La Marina Cdra. 36 S/N Distrito La Perla, Provincia Constitucional del Callao
Teléfono:	:	207-8900 Anexo 2912
Correo electrónico:	:	daniel.uriona@marina.pe felix.buendia@marina.pe eduardo.estacio@marina.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del "SERVICIO DE RENOVACIÓN DE LICENCIAMIENTO DE SOFTWARE DE LA PLATAFORMA DE SERGURIDAD/SERVICIO PP-0135"

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Resolución Jefatural N° 085-2021 JESUETEL de fecha 23 de junio del 2021.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Directamente Recaudados.

Importante

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

1.5. SISTEMA DE CONTRATACIÓN

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

1.6. DISTRIBUCIÓN DE LA BUENA PRO

No aplica.

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 establecido en cada uno de los ítems detallado en el capítulo III de las presentes bases y en concordancia con lo establecido en el expediente de contratación.

1.9. COSTO DE REPRODUCCIÓN Y ENTREGA DE BASES

Los participantes registrados tienen el derecho de recabar un ejemplar de las bases gratuito, a requerimiento del participante se le entregará vía digital.

Importante

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

1.10. BASE LEGAL

- DECRETO DE URGENCIA Nº 014-2019, Decreto de Urgencia de Presupuesto del Sector Público para el Año Fiscal 2020.
- DECRETO DE URGENCIA Nº 015-2019, Decreto de Urgencia de Presupuesto del Sector Público para el Año Fiscal 2020 Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2020.
- DECRETO DE URGENCIA Nº 016-2019, Decreto de Urgencia para el endeudamiento del sector público para el año fiscal 2020.
- Ley N° 30225, Ley de Contrataciones del Estado, y sus modificatorias.
- Decreto Supremo N° 168-2020 EF Modifica el Reglamento de la Ley N° 30225, Ley de Contrataciones del Estado, aprobado mediante Decreto Supremo N° 344-2018-EF.

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

CAPÍTULO II
DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CALENDARIO DEL PROCEDIMIENTO DE SELECCIÓN

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

Importante

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

2.2. CONTENIDO DE LAS OFERTAS

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

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

a) Declaración jurada de datos del postor. **(Anexo 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.

El certificado de vigencia de poder expedido por registros públicos no debe tener una antigüedad mayor de treinta (30) días calendario a la presentación de ofertas, computada desde la fecha de emisión.

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 Catalogo de Servicios de dicha plataforma, no corresponderá exigir el certificado de vigencia de poder y/o documento nacional de identidad.

[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/

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

d) Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. **(Anexo N° 3)**

e) Declaración jurada de plazo de prestación del servicio. **(Anexo N° 4)**[4]

f) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. **(Anexo N° 5)**

g) El precio de la oferta en SOLES debe registrarse directamente en el formulario electrónico del SEACE.

h) Fichas técnicas, en idioma original, de los equipos de red propuestos en la oferta, señalando la marca y modelo.

Adicionalmente, se debe adjuntar el Anexo N° 6 en el caso de procedimientos convocados a precios unitarios, esquema mixto de suma alzada y precios unitarios, porcentajes u honorario fijo y comisión de éxito, según corresponda.

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

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

Importante

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

2.2.1.2. Documentos para acreditar los requisitos de calificación

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

2.2.2. Documentación de presentación facultativa:

a) En el caso de microempresas y pequeñas empresas integradas por personas con discapacidad, o en el caso de consorcios conformados en su totalidad por estas empresas, deben presentar la constancia o certificado con el cual acredite su inscripción en el Registro de Empresas Promocionales para Personas con Discapacidad[5].

b) Solicitud de bonificación por tener la condición de micro y pequeña empresa. **(Anexo N° 11)**

[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.

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

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

Advertencia

El órgano encargado de las contrataciones o el comité de selección, según corresponda, no podrá exigir al postor la presentación de documentos que no hayan sido indicados en los acápites "Documentos para la admisión de la oferta", "Requisitos de calificación" y "Factores de evaluación".

2.3. PRESENTACIÓN DEL RECURSO DE APELACIÓN

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

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

N ° de Cuenta	:	0000-283975
Banco	:	BANCO DE LA NACIÓN
N° CCI[6]	:	018-000-000000283975-01

2.4. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

a) Garantía de fiel cumplimiento del contrato mediante carta fianza.
b) Garantía de fiel cumplimiento por prestaciones accesorias, de ser el caso, mediante Carta fianza.
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 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[7] 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) Detalle de los precios unitarios del precio ofertado[8].
i) Estructura de costos[9].

[6] En caso de transferencia interbancaria.

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

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

[9] Incluir solo cuando resulte necesario para la ejecución contractual, identificar los costos de cada uno de los rubros que

j) Detalle del precio de la oferta de cada uno de los servicios que conforman el paquete[10].
k) Declaración Jurada de Compromiso ANTISOBORNO. **(Según formato Adjunto anexo (12).**
l) Declaración Jurada de no tener impedimento para contratar con el estado **(Según formato adjunto anexo (13).**
m) Copia del voucher o carta emitida por una Entidad Bancaria y/o Compañía de Seguro donde figure la razón social y/o nombre de la persona natural donde figure el código de cuenta interbancaria.

Importante

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

- *En los contratos 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 original, 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. 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 cuyos montos sean iguales o menores a cien mil Soles (S/ 100,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias. Dicha excepción también aplica a los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados no supere el monto señalado anteriormente, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*

Importante

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

- *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya[11].*

comprenden la oferta.

[10] Incluir solo en caso de contrataciones por paquete.

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

- *La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.*

2.5. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en la Dirección de Telemática de la Marina, ubicado en la Av. La Marina Cdra. 36 S/N Distrito La Perla – Callao.

2.6. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en el periodo de vigencia del contrato, dichos pagos serán de la manera indicada en cada uno de los ítems descritos en el capítulo III.

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

- Acta de conformidad del Jefe del Departamento de Administración de Redes y Ciberseguridad de la Dirección de Telemática de la Marina, emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago.

Dicha documentación se debe presentar en la la Dirección de Telemática de la Marina, ubicado en la Av. La Marina Cdra. 36 S/N Distrito La Perla – Callao.

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

ÍTEM N°1

SERVICIO DE LICENCIAMIENTO PARA EL SISTEMA DE SEGURIDAD INFORMÁTICA DE FIREWALL PERIMETRAL Y RED PRIVADA VIRTUAL (VPN)

I. TÉRMINOS DE REFERENCIA

1. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de renovación de licenciamiento para el sistema de seguridad informática de Firewall Perimetral y Red Privada VPN.

2. FINALIDAD PÚBLICA

La Marina de Guerra del Perú requiere renovar la licencia del sistema de seguridad informática firewall perimetral para incrementar los niveles de seguridad de la red WAN Naval, el licenciamiento a adquirirse deberá de contar con la capacidad de satisfacer las necesidades requeridas por la Institución.

3. ANTECEDENTES

La Entidad, dentro de su estrategia de seguridad de la información institucional, posee un conjunto de soluciones de seguridad informática que permiten proteger la información que se encuentra almacenada en los diferentes equipos informáticos, estaciones de trabajo y servidores.

En tal sentido, el presente proceso se enfoca en renovar y continuar brindando la seguridad multifuncional de cara a internet, lo cual se obtiene al ubicar un firewall UTM en el perímetro, controlando, analizando y filtrando todo el acceso del tráfico entrante y saliente.

4. OBJETIVO DE LA CONTRATACIÓN

Mantener el nivel de seguridad de la información de la Entidad a través de la renovación de licenciamiento para el sistema de seguridad informática de Firewall Perimetral y Red Privada VPN con capacidad para soportar al menos 25 Gbps y en configuración de alta disponibilidad.

5. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

5.1. Actividades

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

Las siguientes actividades serán realizadas en forma anual, en cumplimiento a la contratación del servicio y en coordinación con la Dirección de Telemática de la Marina, en adelante DIRTEL:

5.1.1. Generación de las licencias correspondientes a la solución de firewall perimetral tipo UTM y recepción por la DIRTEL.
5.1.2. Instalación y/o configuración de la solución propuesta de ser requerido.
5.1.3. Instalación de la nueva licencia en la solución.
5.1.4. Revisión y/u optimización integral de la solución.

5.2. Recursos a ser provistos por el proveedor

5.2.1. TRES (3) licenciamientos anuales (vigencia de 365 días cada uno) de la solución de firewall perimetral tipo UTM, que incluye consola de gestión y reportador, con capacidad para soportar al menos 25 Gbps y alta disponibilidad, a nombre de la Marina de Guerra del Perú.
5.2.2. La solución de firewall perimetral tipo UTM presentará alta disponibilidad tipo cluster.
5.2.3. Las características básicas de la solución de firewall perimetral tipo UTM serán las siguientes:

5.2.3.1. El licenciamiento deberá permitir un rendimiento de al menos 7 Gbps de prevención de amenazas medidos con tráfico Empresarial Mixto o Condiciones de Prueba Empresarial.
5.2.3.2. El licenciamiento deberá permitir el funcionamiento de fuentes redundantes
5.2.3.3. El licenciamiento deberá permitir el almacenamiento local de al menos 240 GB.
5.2.3.4. El licenciamiento deberá permitir el uso de al menos 8 interfaces GE, 2 SFP+ y 2 SFP.
5.2.3.5. El licenciamiento deberá permitir al menos 8M de conexiones concurrentes.
5.2.3.6. El licenciamiento deberá permitir el uso de una interfaz GE para administración dedicada.
5.2.3.7. El licenciamiento deberá permitir operar simultáneamente en modo sniffer (monitoreo y análisis de tráfico de red), capa 2 (L2) y capa 3 (L3).
5.2.3.8. Debe ser compatible con NAT estático y NAT dinámico
5.2.3.9. Para IPv4, soportar enrutamiento estático y dinámico (RIP, OSPF y BGP) Interface gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interface debe soportar SSL sobre HTTP (HTTPS)
5.2.3.10. Comunicación cifrada y autenticada con username y password, tanto como para la interface gráfica de usuario como la consola de administración de línea de comandos (SSH)
5.2.3.11. El administrador del sistema soporta las opciones incluidas de autenticarse vía password y vía certificados digitales.
5.2.3.12. Deberá ofrecer la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet, http o HTTPS.
5.2.3.13. Soporte de SNMP versión 2
5.2.3.14. Soporte de syslog para poder enviar bitácoras a servidores de SYSLOG remotos.
5.2.3.15. Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 2 perfiles para administración y monitoreo del Firewall.
5.2.3.16. Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.
5.2.3.17. Debe soportar el protocolo estándar de la industria VXLAN;
5.2.3.18. Debe incluir capacidades de SD-WAN perpetuas o licenciadas durante el periodo de tres años.

5.2.3.19. En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN.
5.2.3.20. Debe soporta protección contra la suplantación de identidad (anti-spoofing);
5.2.3.21. Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs
5.2.3.22. Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.
5.2.3.23. Las reglas del firewall deberán tomar en cuenta dirección IP fuente (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
5.2.3.24. El análisis de firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;
5.2.3.25. Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación
5.2.3.26. Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.
5.2.3.27. Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año)
5.2.3.28. Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.
5.2.3.29. Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.
5.2.3.30. Deberá soportar reglas de firewall en IPv6.
5.2.3.31. Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP
5.2.3.32. Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs
5.2.3.33. Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas
5.2.3.34. Soportar Policy based routing o policy based forwarding;
5.2.3.35. El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál de tráfico sale por un enlace y qué tráfico sale por otro enlace
5.2.3.36. Soporte a ruteo dinámico RIP, OSPF y BGP
5.2.3.37. Soporte a ruteo de multicast
5.2.3.38. Soportar alta Disponibilidad en modo Activo-Pasivo/Activo-Activo
5.2.3.39. Posibilidad de definir al menos dos interfaces para sincronía de Cluster
5.2.3.40. La configuración de alta disponibilidad debe sincronizar: sesiones, configuraciones, incluyendo, políticas de Firewalls, NAT, QoS y objetos de la red;
5.2.3.41. La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;
5.2.3.42. La configuración de alta disponibilidad debe sincronizar: Tablas FIB;
5.2.3.43. Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);
5.2.3.44. Debe soportar la integración con otras plataformas de ciberseguridad a través de API, a fin de proporcionar una solución integral que proteja diferentes vectores de ataque;
5.2.3.45. Debe soportar integración con una plataforma de sandboxing en las instalaciones de la misma marca, para detectar amenazas avanzadas dentro de la red.

5.2.3.46. La solución debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.
5.2.3.47. Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto país/países;
5.2.3.48. Debe permitir la visualización de los países de origen y destino en los registros de acceso;
5.2.3.49. Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;
5.2.3.50. Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);

5.2.4. Las características específicas de la solución de firewall perimetral tipo UTM relacionados a la identificación de usuarios serán los siguientes:

5.2.4.1. Capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;
5.2.4.2. Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;
5.2.4.3. Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;
5.2.4.4. Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la política/control basados en usuarios y grupos de usuarios;
5.2.4.5. Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autentificación residente en el equipo de seguridad (portal cautivo);
5.2.4.6. Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;
5.2.4.7. Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;
5.2.4.8. Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;

5.2.5. Las características específicas de la solución de firewall perimetral tipo UTM para la función de control de aplicaciones serán los siguientes:

5.2.5.1. Reconocer miles de aplicaciones diferentes, distribuido en 18 categorías, incluyendo: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, video, Proxy, mensajería instantánea, compartición de archivos, correo electrónico.
5.2.5.2. La solución deberá tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo.
5.2.5.3. Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través

de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor.

5.2.5.4. Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante
5.2.5.5. Actualización de la base de firmas de la aplicación de forma automática.
5.2.5.6. Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas.
5.2.5.7. Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante.
5.2.5.8. Debe alertar al usuario cuando sea bloqueada una aplicación.
5.2.5.9. Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
5.2.5.10. Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación y categoría de Aplicación

5.2.6. Las características específicas de la solución de firewall perimetral tipo UTM para la función de filtrado URL serán los siguientes:

5.2.6.1. Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora).
5.2.6.2. Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad.
5.2.6.3. Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory y la base de datos local.
5.2.6.4. Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local.
5.2.6.5. Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL.
5.2.6.6. Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL.
5.2.6.7. Tener por lo menos 60 categorías de URL.
5.2.6.8. Debe tener la funcionalidad de exclusión de URLs por categoría.
5.2.6.9. Permitir página de bloqueo personalizada.
5.2.6.10. Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio).

5.2.7. Las características específicas de la solución de firewall perimetral tipo UTM para la función de prevención de amenazas serán los siguientes:

5.2.7.1. Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo.
5.2.7.2. Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware).
5.2.7.3. Las características de IPS, antivirus y anti-spyware deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante
5.2.7.4. Debe ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

5.2.7.5. Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas.
5.2.7.6. Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos.
5.2.7.7. Deber permitir el bloqueo de vulnerabilidades y de exploits conocidos.
5.2.7.8. Debe incluir la protección contra ataques de denegación de servicio.
5.2.7.9. Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc.
5.2.7.10. Detectar y bloquear los escaneos de puertos de origen.
5.2.7.11. Bloquear ataques realizados por gusanos (worms) conocidos.
5.2.7.12. Contar con firmas específicas para la mitigación de ataques DoS y DDoS.
5.2.7.13. Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow).
5.2.7.14. Debe poder crear firmas personalizadas
5.2.7.15. Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3.
5.2.7.16. Soportar el bloqueo de archivos por tipo.
5.2.7.17. Identificar y bloquear la comunicación con redes de bots.
5.2.7.18. Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación.
5.2.7.19. La solución debe proteger de amenazas avanzadas que utilizan conexiones DNS, de manera que permita filtrar las consultas de DNS de los hosts para bloquear conexiones hacia sitios maliciosos, conexiones de botnet, ya sea en base a categorías o firmas.
5.2.7.20. La capacidad de filtro de DNS debe ser alimentada por un servicio de inteligencia de amenazas de la propia marca.
5.2.7.21. Debe permitir la translación en el firewall de una consulta de DNS, a fin de redirigir la resolución hacia otro destino diferente del original.
5.2.7.22. Los eventos deben identificar el país que origino la amenaza;
5.2.7.23. Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms).
5.2.7.24. Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP.
5.2.7.25. La solución debe permitir coordinar el estado observado por el software de seguridad endpoint con las acciones que toma el firewall a nivel de red;
5.2.7.26. Proporcionar protección contra ataques de día cero a través de una estrecha integración con componentes de red de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube).

5.2.8. Las características específicas de la solución de firewall perimetral tipo UTM para la función VPN serán los siguientes:

5.2.8.1. Soporte VPN de sitio-a-sitio y cliente-a-sitio.
5.2.8.2. Soportar VPN IPSec y VPN SSL.
5.2.8.3. La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512.
5.2.8.4. La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
5.2.8.5. La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2).
5.2.8.6. La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
5.2.8.7. Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución
5.2.8.8. Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
5.2.8.9. Las características de VPN SSL se deben cumplir con o sin el uso de agentes.

5.2.8.10. Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy.
5.2.8.11. Asignación de DNS en la VPN de cliente remoto.
5.2.8.12. Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL.
5.2.8.13. Suportar autenticación vía AD/LDAP, token, certificado y base de usuarios local.
5.2.8.14. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
5.2.8.15. Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;
5.2.8.16. Deberá mantener una conexión segura con el portal durante la sesión;
5.2.8.17. La capacidad de conexión VPN SSL o IPSEC cliente-a-sitio debe disponer de un agente con compatibilidad al menos para Windows, Mac OS, android y iOS. Además, debe contar con un método de conexión que no requiera de un agente instalado.
5.2.8.18. La plataforma debe tener la capacidad de soportar al menos 7,000 conexiones VPN SSL concurrentes desde dispositivos endpoint y móviles, ya sea usando agente o sin agente.
5.2.8.19. El agente de VPN client-to-site debe validar la configuración del dispositivo cliente antes de otorgar el acceso a la red. Debe soportar como mínimo los siguientes criterios de evaluación antes de brindar el acceso a la red: protección activa del antivirus, firewall de host y versión de sistema operativo, así como una combinación de estos criterios.
5.2.8.20. Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;
5.2.8.21. La solución debe considerar al menos dos tokens, permitiendo la autenticación de dos factores para los usuarios asignados hacia la interfaz de gestión del firewall y el acceso por VPN SSL;

5.2.9. Las características específicas de la solución de firewall perimetral tipo UTM para la función "QoS traffic shaping" serán los siguientes:

5.2.9.1. Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming.
5.2.9.2. Soportar la creación de políticas de QoS y Traffic Shaping:
a. Por dirección de origen.
b. Por dirección de destino.
c. Por usuario y grupo.
d. Por aplicaciones.
5.2.9.3. Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto.
5.2.9.4. En QoS debe permitir la definición de tráfico con ancho de banda garantizado y máximo ancho de banda.
5.2.9.5. En QoS debe permitir la definición de colas de prioridad.
5.2.9.6. Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.
5.2.9.7. Soportar marcación de paquetes DiffServ, incluso por aplicación.
5.2.9.8. Soportar la modificación de los valores de DSCP para Diffserv.
5.2.9.9. Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service).
5.2.9.10. Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shaping.

5.2.9.11. Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes.

5.2.10. Las características específicas de la solución de firewall perimetral tipo UTM referidos a la generación de reportes serán los siguientes:

5.2.10.1. El licenciamiento deberá permitir el que la consola de reportes pueda almacenar al menos 100 GB de Logs por día.
5.2.10.2. Deberá permitir el almacenamiento de al menos 7.5 TB.
5.2.10.3. Soporte de colección de eventos de Syslog
5.2.10.4. Capacidad de generar reportes en formato PDF, HTML, CSV y XML
5.2.10.5. Poseer más de 50 plantillas de reportes listas para uso.
5.2.10.6. Capacidad de envío de reportes por correo electrónico.
5.2.10.7. Capacidad de reenviar los eventos en formato CEF (Common Event Format) a un equipo externo
5.2.10.8. Capacidad de creación de perfiles de acceso multi-tennat permitiendo que la información de los dispositivos sea aislado.
5.2.10.9. Deberá soportar licenciamiento futuro para la visualización de Indicadores de Compromiso IOC.

5.2.11. Las características específicas de la solución de firewall perimetral tipo UTM referidos a la consola de software tokens serán los siguientes:

5.2.11.1. Permitir el despliegue de Máquina virtual para la administración de al menos 1000 software Tokens, los mismos que serán proporcionados a la Entidad.
5.2.11.2. Soportar la implementación en plataformas de virtualización VMware ESXi 6.0 / 6.5, Microsoft Hyper-V 2012 R2 / 2016 y Xen
5.2.11.3. Soportar la administración de la interfaz gráfica de usuario (GUI) a través de HTTP y / o HTTPS
5.2.11.4. Soportar la administración de la interfaz basada en la línea de comandos (CLI) a través de TELNET y / o SSH
5.2.11.5. Permitir definir perfiles de administrador para la solución, de manera que pueda segmentar la responsabilidad de los administradores por tareas operativas
5.2.11.6. Tener un indicador visual centralizado de información crítica (estado de la licencia, versión de firmware, consumo de CPU / memoria / disco, número de usuarios creados y con licencia)
5.2.11.7. Soportar la actualización de firmware a través de una interfaz gráfica, mediante un proceso simplificado e intuitivo
5.2.11.8. Soportar la personalización de mensajes de soluciones estándar, como páginas de error, portales de autenticación, registro automático, restablecimiento de contraseña y otros.
5.2.11.9. Soportar la opción de copia de seguridad encriptada
5.2.11.10. Soportar copias de seguridad automatizadas (programadas según criterios predefinidos), no solo bajo demanda
5.2.11.11. Soportar una copia de seguridad de la configuración completa, incluida la base de usuarios, grupos, tokens, certificados, configuraciones de inicio de sesión único, etc. La solución también debe permitir restaurar toda la configuración directamente desde la interfaz gráfica.
5.2.11.12. Soporta SNMP v1, v2 y v3 permitiendo consultar su propia MIB y enviar Traps
5.2.11.13. Soportar la captura de paquetes a través de GUI para la resolución de problemas avanzada en herramientas de análisis de paquetes (por ejemplo, Wireshark)
5.2.11.14. El equipo debe permitir el envío de correos electrónicos relacionados con el restablecimiento de contraseña, aprobación de nuevos usuarios, autorregistro de usuario y autenticación de segundo factor (token)

5.2.11.15. Apoyar el registro de todos los eventos que los usuarios de su base de datos local realizan con sus cuentas, como crear un usuario, cambiar la contraseña de un usuario y cambiar la información general.
5.2.11.16. Debe poder integrarse con un directorio activo (Windows AD) y poder ofrecer funcionalidad SSO, donde la autenticación automática / transparente a través de SSO para los servicios necesarios se basa en la autenticación previa realizada por el usuario en el dominio.
5.2.11.17. Debería permitir definir una lista de usuarios de SSO que serán ignorados, evitando así la interferencia de cuentas de servicio como antivirus o scripts a través de GPO.
5.2.11.18. Debe admitir el análisis de archivos syslog enviados desde una fuente remota, para que los utilice el servicio SSO.
5.2.11.19. Debe admitir el lenguaje de marcado de aserción de seguridad (SAML), actuando como un autenticador de un proveedor de servicios (SP) que solicita información de identidad de usuario de proveedores de identidad de terceros (IDP)
5.2.11.20. Debe admitir SSO basado en Radius (RSSO - RADIUS Single Sign-On)
5.2.11.21. Debe ser compatible con el proxy de contabilidad RSSO que permite la recepción de paquetes de radio de transmisión, la modificación de estos paquetes y su reenvío a varios otros puntos.
5.2.11.22. Debe realizar la autenticación para la gestión de la identidad de los usuarios de la red, ayudando a simplificar su administración, siendo un punto central de control de autenticación, donde se pueden consolidar múltiples métodos de autenticación.
5.2.11.23. Debe soportar licenciamiento futuro para la autenticación de dos factores en al menos dos tipos diferentes de tokens, el primero es físico (token) y el segundo lógico como software para dispositivos móviles, correo electrónico o SMS, lo que permite elegir cuál de los tipos usar para cada uno. usuario.
5.2.11.24. Debe permitir la definición de un perfil de complejidad mínima para las contraseñas de todos los usuarios registrados en la base de datos local, permitiendo la definición de un número mínimo de letras minúsculas, mayúsculas, caracteres numéricos, caracteres.
5.2.11.25. Debe permitir la creación de una política de bloqueo automático de usuarios después de una serie de fallas de autenticación, evitando así ataques de fuerza bruta.
5.2.11.26. Debe admitir la creación de usuarios a nivel local, que se pueden utilizar para autenticar los dispositivos según sea necesario.
5.2.11.27. Debe permitir la creación masiva de usuarios en la base de datos local mediante la importación de una lista de usuarios que se creará contenida en archivos externos.
5.2.11.28. Debe permitir la creación de nuevos usuarios en la base de datos local y que el creador / administrador pueda establecer una contraseña al momento de crearla.
5.2.11.29. Debe permitir la creación de nuevos usuarios en la base de datos local para que el equipo genere una contraseña aleatoria y la envíe automáticamente al usuario.
5.2.11.30. Debe permitir la creación de nuevos usuarios en la base de datos local sin establecer una contraseña, requiriendo que utilicen el token como único factor de autenticación.
5.2.11.31. Debe permitir asociar tokens a usuarios creados localmente en la base de datos.
5.2.11.32. Debe permitir a los usuarios registrar sus tokens e informar la pérdida de un token automáticamente, sin la necesidad de involucrar a un administrador.
5.2.11.33. Debe tener formas que permitan a los usuarios locales restablecer sus contraseñas de forma segura sin la intervención de los administradores, por correo electrónico o preguntas de seguridad.

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

5.2.11.34. Debe admitir la creación de grupos de usuarios, que se pueden utilizar en la autenticación de dispositivos según sea necesario
5.2.11.35. Los tokens deben generar códigos con al menos 6 dígitos e intervalos que no excedan los 60 segundos
5.2.11.36. Soporta autenticación de dos factores por aplicación móvil (iPhone y Android)
5.2.11.37. Soporta la autenticación de dos factores mediante el envío de correo electrónico.
5.2.11.38. Debe permitir deshabilitar un token cuando es robado o perdido, permitiendo su posterior reactivación cuando se recupera
5.2.11.39. Debe permitir la disociación de un token de un usuario y asociarlo con otro usuario cuando sea necesario, permitiendo así su reutilización.
5.2.11.40. Debe continuar permitiendo la autenticación de dos factores en los clientes de Windows incluso con la máquina fuera de línea
5.2.11.41. Debe proporcionar un portal web para el autorregistro de los usuarios, para que puedan acceder, completar sus datos y enviar el registro. Después de que el usuario se registra, el administrador debe ser notificado automáticamente para aprobar o denegar su registro antes de que se active.
5.2.11.42. Debe funcionar como un servidor RADIUS (Servidor de usuario de acceso telefónico de autenticación remota), proporcionando autenticación a los dispositivos compatibles con este protocolo.
5.2.11.43. Debe funcionar como un servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticación a los dispositivos que admiten este protocolo.
5.2.11.44. Debe contar con un servidor LDAP interno que permita su configuración jerárquica, para una correcta administración por grupos o unidades organizativas de usuarios locales.
5.2.11.45. Debe admitir la integración del servidor LDAP remoto (como Microsoft Active Directory)
5.2.11.46. Debe permitir a los usuarios que no tienen una cuenta local o de redes sociales autenticarse mediante un registro rápido, que garantiza un mínimo de trazabilidad, mediante la validación de direcciones de correo electrónico o números de teléfono
5.2.11.47. Debe permitir el inicio de sesión automático de los usuarios invitados después de que se hayan registrado correctamente.
5.2.11.48. Debe admitir el lenguaje de marcado de aserción de seguridad (SAML), actuando como un proveedor de identidad (IDP) que establece una relación de confianza para la autenticación segura de los usuarios que intentan acceder a un proveedor de servicios (SP).

5.2.12. Con la finalidad que el proveedor cumpla con proporcionar una solución de solución de firewall perimetral tipo UTM de acuerdo a las exigencias técnicas requeridas en el presente documento durante el plazo establecido, se aceptará la reposición y/o inclusión de hardware tipo appliance necesario. Para tal efecto, se deberá tener en cuenta las diferentes vigencias tecnológicas publicadas por el fabricantes en sus canales de comunicación oficiales.
5.2.13. El proveedor proveerá los materiales tipo cableado, conectores u otros necesarios para el cumplimiento de las actividades tipificadas en el numeral 5.1, en coordinación con la DIRTEL.

5.3. Recursos y facilidades a ser provistos por la Entidad

5.3.1. La Jefatura del Departamento de Administración de Redes y Ciberseguridad brindará las facilidades y accesos para el cumplimiento del servicio requerido.
5.3.2. La Entidad brindará una máquina virtual para la instalación de la solución de doble factor del VPN en coordinación con la DIRTEL. Dicha máquina virtual deberá poseer las siguientes características: 2 vCPU , 4GB de RAM y 500GB de disco.

5.4. Reglamentos sanitarios nacionales

El personal de la empresa adjudicada, que tengan contacto y/o realice actividades de distinta índole (tramite documentario, entrega de material, abastecimiento, brindar servicios o prestaciones, entre otros), dentro de las instalaciones de la Marina de Guerra del Perú, emitirán Declaración Jurada de toma de conocimiento y cumplimiento a los protocolos sanitarios siguientes:

5.4.1. Aislamiento COVID-19.- Procedimiento a responsabilidad de las empresas adjudicadas u otras actividades de distinta índole, por el cual una persona con caso sospechoso, reactivo en la prueba rápida o positivo en la Prueba PCR para COVID-19 será aislado y evacuado en forma inmediata al Centro de Salud para su evaluación correspondiente, debiendo elevar el respectivo informe médico por el postor adjudicado, donde se detallará las indicaciones dadas por la parte médica y su alta médica respectiva.

5.4.2. Distanciamiento Social.- Aumentar el espacio que separa a las personas y reducir la frecuencia de contacto, con el fin de reducir la transmisión de la enfermedad (distancia mínima de DOS (2) metros aproximadamente.

5.4.3. Higiene Respiratoria. - Cubrirse la boca y nariz con UNA (1) tapa boca certificado y aprobado por el MINSA, en todo momento y de manera obligatoria.

5.4.4. Higiene de manos.- Uso de guantes y lavado de manos a menudo con agua y jabón o solución recomendada; de acuerdo a la naturaleza de su visita, de manera obligatoria.

5.4.5. Higiene Ambiental. Mantener la limpieza de los lugares, superficies y movilidades de trabajo, de manera constante y obligatoria.

Asimismo, los postores deberán presentar declaración jurada donde se detalle que el personal a su cargo no presenta sintomatología o haber estado en contacto de personas infectadas con COVID-19, con el propósito de descartar cualquier contagio del personal de la Marina de Guerra del Perú, el postor dará cumplimiento a dispuesto en la Resolución Nº 283-2020 MINSA de fecha 13 de mayo del 2020, en lo referente a trabajadores con riesgo y alto riesgo a exposición COVID-19, donde se detalla al personal vulnerable las características de este tipo de personas, las cuales son:

- Mayores de 65 años
- Embarazadas y lactantes
- Enfermos cardiovasculares
- Pacientes con cáncer y/o diabetes mellitus
- Obesos con IMC de 40 a mas
- Asmáticos moderados o graves
- Enfermos respiratorios crónicos
- Enfermos pulmonares crónicos
- Insuficientes renales crónicos en tratamientos con hemodiálisis
- Enfermos o en tratamiento con inmunosupresores
- Otros, bajo responsabilidad del postor adjudicado.

Se aplicará lo establecido según Resolución Ministerial Nro. 265-2020 MINSA de fecha 7 de mayo del 2020, modificada por Resolución Ministerial Nro. 283-2020 MINSA de fecha 13 de mayo del 2020.

5.5. Prestaciones accesorias a la prestación principal

5.5.1. Mantenimiento preventivo

5.5.1.1. Se podrá requerir el mantenimiento preventivo de la solución de firewall perimetral tipo UTM en forma semestral y en coordinación con la Dirección de Telemática de la Marina.

5.5.2. Soporte técnico

5.5.2.1. Se podrá requerir soporte técnico vía telefónica, correo electrónico o sesión remota, tipo 24x7x365, es decir durante las 24 horas del día, los 7 días de la semana y los 365 días del año, con un tiempo máximo de respuesta de 4 horas. En caso no se pudiera solucionar un incidente a través de los medios antes descritos luego de 48 horas de transcurrido el incidente, el soporte técnico deberá realizarse en forma presencial.

5.5.2.2. Deberá asegurarse el acceso permanente y oportuno a las actualizaciones de seguridad y de rendimiento de la solución de firewall perimetral tipo UTM ofertado, parcial o integral, proporcionado por el fabricante.

5.5.2.3. Se podrá requerir evaluaciones de mejora y/o prevención para la solución de firewall perimetral tipo UTM, parcial o integral.

5.5.2.4. Se podrá requerir la ejecución de un ASSESSMENT DE SEGURIDAD con una herramienta de pentesting a la solución de firewall perimetral tipo UTM por única vez y en forma coordinada con la Dirección de Telemática de la Marina.

5.5.2.5. Efectuará el escalamiento de soporte a nivel fabricante cuando lo requiera la Dirección de Telemática de la Marina.

5.5.2.6. Deberá proporcionar alternativas de solución para no afectar la continuidad del servicio por un plazo no mayor a 72 horas a partir del inicio del incidente.

5.5.3. Capacitación

5.5.3.1. Se podrá requerir la capacitación en administración de la solución de firewall perimetral tipo UTM, el cual estará dirigido a un mínimo de TRES (3) técnicos de la División de Ciberseguridad de la DIRTEL, con un tiempo mínimo de duración de 8 horas, a realizarse en las instalaciones de la Entidad, o en forma virtual, dentro de los 3 meses posteriores a la culminación de las actividades tipificadas en el numeral 5.1.

5.5.3.2. El sylabus corresponderá a la versión de la solución de firewall perimetral tipo UTM implementada y será elaborado por el proveedor en coordinación con la DIRTEL.

5.5.3.3. El material a entregar deberá contemplar el detalle de todos los temas a dictarse según el sylabus.

5.5.3.4. Se deberá otorgar constancias de participación para el personal que siga la capacitación.

5.5.4. Garantía

5.5.4.1. El proveedor presentará la garantía de buen funcionamiento será por el mismo periodo de vigencia del licenciamiento. Asimismo, iniciará al mismo tiempo que la vigencia del licenciamiento del software de seguridad implementado por el proveedor.

5.5.4.2. La garantía de buen funcionamiento comprende que la solución ofertada cumpla con todos los requerimientos tipificados en el presente documento.

5.6. Lugar y plazo de la prestación

5.6.1. Lugar

La prestación del servicio será en la Dirección de Telemática de la Marina, cito en Av. La Marina Cdra. 36 S/N, dentro de la Estación Naval La Perla.

5.6.2. Plazo

5.6.2.1. El plazo para la configuración del servicio del periodo comprendido entre los años 2021 - 2022, será de 50 días calendario, contabilizados a partir del día siguiente de la firma del contrato.
5.6.2.2. La configuración del servicio del periodo comprendido entre los años 2022 – 2023 y 2023 - 2024, será de máximo 10 días calendarios antes de la caducidad de la licencia vigente.
5.6.2.3. El plazo de ejecución del servicio es de 1,095 días calendarios, dividido en tres periodos de 365 días calendarios entre los años 2021 y 2024, los mismos que corresponden a la duración del licenciamiento anual a ser expedidas.

5.7. Confidencialidad

El POSTOR deberá firmar el Acta de Confidencialidad proporcionado por la Dirección de Telemática de la Marina, para el desarrollo de los trabajos de soporte técnico y otros que se realicen sobre los sistemas informáticos de la Institución, el cual se realizará a la firma del contrato.

El acuerdo de confidencialidad formará parte del contrato a fin de permitir y resguardar la información clasificada de la Institución, pudiéndose limitar el acceso de profesionales que puedan afectar a la seguridad de la Institución.

5.8. Medidas de control durante la ejecución contractual

5.8.1. Designación de responsabilidades

5.8.1.1. Áreas que coordinarán con el proveedor: La Jefatura del Departamento de Administración de Redes y Ciberseguridad y la División de Ciberseguridad.
5.8.1.2. Área responsable de las medidas de control: La Jefatura del Departamento de Administración de Redes y Ciberseguridad.
5.8.1.3. Área que brindará la conformidad: La Jefatura de la División de Ciberseguridad.

5.8.2. Medidas de control

5.8.2.1. Supervisará que el proveedor cumpla con todo lo requerido en el presente documento.
5.8.2.2. Verificará la correcta confección del Acta de Conformidad.

5.8.3. Conformidad

Se elaborarán Actas de Conformidad en forma anual, posterior a la configuración del servicio de licenciamiento requerido, debiendo contener los siguientes documentos:

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

5.8.3.1. Screenshot del portal oficial del fabricante donde figuren las claves u otros indicadores que permita validar la licencia proporcionada.
5.8.3.2. Informe elaborado por el proveedor donde acredite el cumplimiento de lo tipificado en el numeral 5.1.
5.8.3.3. Declaración jurada del proveedor en el cual se compromete a brindar el mantenimiento preventivo, soporte técnico, capacitación y garantía de buen funcionamiento, de acuerdo a lo tipificado del numeral 5.5.1 al numeral 5.5.4. En dicho documento el proveedor deberá indicar los teléfonos y correos electrónicos para contacto.

5.9. Forma de pago

El pago se realizará en TRES (03) armadas, previa presentación del acta de conformidad detallada en el numeral 5.9.3, de acuerdo a lo siguiente:

5.9.1. El primer pago se efectuará en el año 2021 y corresponderá al 33.33% del monto contractual.
5.9.2. El segundo pago se efectuará en el año 2022 y corresponderá al 33.33% del monto contractual.
5.9.3. El segundo pago se efectuará en el año 2023 y corresponderá al 33.34% del monto contractual.

ÍTEM N°2

SERVICIO DE LICENCIAMIENTO PARA EL SISTEMA DE SEGURIDAD INFORMÁTICA DE FIREWALL DE APLICACIONES WEB (WAF)

I. TÉRMINOS DE REFERENCIA

1. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de licenciamiento para el sistema de seguridad informática de firewall de aplicaciones web (WAF).

2. FINALIDAD PÚBLICA

La Marina de Guerra del Perú, requiere el servicio de protección para las aplicaciones Web implementadas, con la finalidad de brindar y asegurar la seguridad de la información dentro de la Red de la WAN Naval.

3. ANTECEDENTES

La Entidad, dentro de su estrategia de seguridad de la información institucional, posee un conjunto de soluciones de seguridad informática que permiten proteger la información que se encuentra almacenada en los diferentes equipos informáticos, estaciones de trabajo y servidores.

En tal sentido, el presente proceso se enfoca en renovar y continuar brindando seguridad informática a través de la detección de ataques dirigidos a los servidores de aplicaciones de la Institución. Para ello, se cuenta con un equipo appliance denominado firewall de aplicaciones web, el cual protege con características especiales a los sistemas de información críticos para la Institución.

4. OBJETIVO DE LA CONTRATACIÓN

Mantener el nivel de seguridad de la información de la Entidad a través de la renovación del licenciamiento para el sistema de seguridad informática de firewall de aplicaciones web (waf).

5. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

5.1. Actividades

Las siguientes actividades serán realizadas en forma anual, en cumplimiento a la contratación del servicio y en coordinación con la Dirección de Telemática de la Marina, en adelante DIRTEL:

5.1.1. Generación de las licencias correspondientes al appliance firewall de aplicaciones web y la remisión a la DIRTEL.
5.1.2. Instalación y/o configuración de la solución propuesta de ser requerido.
5.1.3. Instalación de la nueva licencia en la solución.
5.1.4. Revisión y/u optimización integral de la solución.

MINISTERIO DE L[illegible]NSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

5.2. Recursos a ser provistos por el proveedor

5.2.1. TRES (3) licenciamientos anuales (vigencia de 365 días cada uno) del equipo appliance firewall de aplicaciones web, a nombre de la Marina de Guerra del Perú.
5.2.2. Las características relacionadas a la protección sobre aplicaciones web que permitirá el licenciamiento sobre el appliance serán las siguientes:

5.2.2.1. El licenciamiento deberá brindar un rendimiento mínimo de 1Gbps.
5.2.2.2. Deberá tener la capacidad de procesamiento SSL basado en hardware.
5.2.2.3. Deberá permitir tener una latencia menor a 5 ms.
5.2.2.4. La solución debe permitir implementación en modo Proxy Transparente, Proxy Reverso y/o Transparente.
5.2.2.5. El firmware debe soportar interfaz gráfica web para la configuración de las funciones del sistema, utilizando navegadores disponibles gratuitamente y protocolo HTTPS, y también por CLI (interfaz de línea de comando), accediendo localmente al equipo por el puerto de consola, o remotamente via SSH.
5.2.2.6. Debe proveer las siguientes informaciones en la interfaz gráfica de gestión: estadísticas de throughput HTTP en tiempo real, estadísticas de eventos de ataques detectados/bloqueados, estadísticas de solicitudes HTTP en tiempo real y los últimos logs de eventos del sistema.
5.2.2.7. La solución deberá de soportar almacenar logs localmente en disco y en servidor externo.
5.2.2.8. La solución debe tener base de datos local que permita la creación de usuarios y permita su uso en la autenticación de los sistemas locales y aplicaciones protegidas.
5.2.2.9. La solución debe tener la capacidad de autenticar usuarios en bases externas remotas: LDAP, RADIUS o SAML.
5.2.2.10. La solución debe proteger contra el Top 10 de ataques a aplicaciones definido por OWASP.
5.2.2.11. La solución debe tener soporte nativo de HTTP/2.
5.2.2.12. La solución debe tener un mecanismo de aprendizaje automático capaz de identificar todos los contenidos de la aplicación, incluyendo URL's, parámetros de URL's, campos de formularios y lo que se espera de cada campo.
5.2.2.13. La solución debe tener la capacidad de protección contra ataques del tipo Adobe Flash binary (AMF).
5.2.2.14. La solución debe tener la capacidad de protección contra ataques del tipo Botnet.
5.2.2.15. La solución debe identificar y proteger contra ataques del tipo Cross Site Request Forgery (CSRF).
5.2.2.16. La solución debe tener funcionalidad de protección contra ataques de cross site scripting (XSS).
5.2.2.17. La solución debe tener la capacidad de protección contra ataques del tipo Local File inclusion (FLI) y Remote File Inclusion (RFI)
5.2.2.18. La solución debe tener la capacidad de protección contra ataques del tipo Man-in-the-middle (MITM).
5.2.2.19. La solución debe tener la capacidad de protección contra ataques del tipo Server Information Leakage.
5.2.2.20. La solución debe contar con protección contra envíos de comandos SQL ocultos en las requisiciones enviadas a la base de datos (SQL Injection).
5.2.2.21. La solución debe tener la capacidad de protección contra ataques del tipo Forms Tampering.
5.2.2.22. La solución debe identificar y proteger contra Zero Day Attacks.
5.2.2.23. La solución debe detectar malware en archivos subidos a través de los servicios web protegidos.
5.2.2.24. Debe incluir la protección contra malware de día cero a través de la integración con análisis Sandbox on-premise o en nube.

5.2.2.25. La solución debe permitir añadir, automáticamente o manualmente, en una lista de bloqueo, las direcciones IP de origen, según la base de IP Reputation.
5.2.2.26. La solución debe soportar SSL/TLS offload para al menos TLS 1.0, 1.1 e 1.2.
5.2.2.27. La solución debe permitir la redirección de solicitudes HTTP para HTTPS.
5.2.2.28. La solución debe tener la capacidad de actuar como un scanner de vulnerabilidades para diagnóstico e identificación de amenazas en los servidores web.

5.2.3. Las caracteristicas relacionadas a las funcionalidades de balanceo de carga serán las siguientes:

5.2.3.1. La solución debe incluir la funcionalidad de balanceo de carga entre servidores web
5.2.3.2. Debe soportar configurar puertos no estándar para aplicación web HTTP y HTTPS
5.2.3.3. Soportar balanceo / distribución de tráfico y enrutear el contenido hacia distintos servidores web
5.2.3.4. La solución debe permitir crear grupos de servidores (Server Farm / Pool) para distribuir las conexiones de los usuarios
5.2.3.5. Soportar el algoritmo Round Robin para balanceo de carga entre servidores
5.2.3.6. Soportar el algoritmo Weighted Round Robin para balanceo de carga entre servidores
5.2.3.7. Soportar el algoritmo Least Connection para balanceo de carga entre servidores
5.2.3.8. La solución debe de soportar creación de servidores virtuales que definan la interfaz de red/bridge y direción IP por donde el tráfico con destino al Server Pool es recibido
5.2.3.9. Los servidores virtuales deben de entregar el tráfico hacia un único servidor web y tambien incluir la opción de distribuir las sessiones/conexiones entre los servidores web del Server Pool
5.2.3.10. Debe de ser porible definir el número máximo de conexiones TCP simultáneas hacia un determinado servidor miembro del Server Pool
5.2.3.11. Permitir prueba de disponibilidad del servidor web a través del método TCP
5.2.3.12. Permitir prueba de disponibilidad del servidor web a través del método ICMP ECHO_REQUEST (ping)
5.2.3.13. Permitir prueba de disponibilidad del servidor web a través del método TCP Half Open
5.2.3.14. Permitir prueba de disponibilidad del servidor web a través del método TCP SSL
5.2.3.15. Permitir prueba de disponibilidad del servidor web a través del método HTTP
5.2.3.16. Permitir prueba de disponibilidad del servidor web a través del método HTTPS
5.2.3.17. En las pruebas de disponibilidad HTTP y HTTPS, permitir indicar la URL exacta a ser probada
5.2.3.18. En las pruebas de disponibilidad HTTP y HTTPS, permitir elegir entre los métodos HEAD, GET y POST
5.2.3.19. En las pruebas de disponibilidad HTTP y HTTPS, permitir elegir el nombre del campo HTTP "host" a ser probado
5.2.3.20. Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Host"
5.2.3.21. Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "URL"
5.2.3.22. Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Parámetro HTTP"
5.2.3.23. Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Referer"

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

5.2.3.24. Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Dirección IP de Origen"
5.2.3.25. Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Encabezado".
5.2.3.26. Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Cookie"
5.2.3.27. Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Valor del campo del Certificado X509"
5.2.3.28. Implementar Cache de Contenido para HTTP, permitiendo que objetos sean almacenados y requisiciones HTTP sean contestadas directamente por la solución
5.2.3.29. La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por dirección IP de origen.

5.2.4. Las características relacionadas a la gestión de logs serán las siguientes:

5.2.4.1. Configurar, administrar y monitorear todos los dispositivos referidos a la solución.
5.2.4.2. Permitir visualizar eventos de tráfico, Bloqueo de Ataques y de Auditoria.
5.2.4.3. Permitir la visualización en tiempo real de los logs de actividad de los equipos de la solución y las modificaciones de configuración que los administradores pudieran efectuar.
5.2.4.4. Permitir la notificación de un determinado evento, producto de la aplicación de una política de seguridad mediante: Email, syslog y traps SNMP, además de su visualización en la consola.

5.2.5. Las características relacionadas a la consola de recolección de eventos críticos y resportes serán las siguientes:

5.2.5.1. Deberá considerarse el licenciamiento para almacenar al menos 100 GB de Logs por día en un equipo dedicado.
5.2.5.2. Deberá permitir el almacenamiento de al menos 7TB.
5.2.5.3. Soporte de colección de eventos de Syslog
5.2.5.4. Capacidad de generar reportes en formato PDF, HTML, CSV y XML
5.2.5.5. Poseer más de 50 plantillas de reportes listas para uso.
5.2.5.6. Capacidad de envío de reportes por correo electrónico.
5.2.5.7. Capacidad de reenviar los eventos en formato CEF (Common Event Format) a un equipo externo
5.2.5.8. Capacidad de creación de perfiles de acceso multi-tennat permitiendo que la información de los dispositivos sea aislada.
5.2.5.9. Deberá soportar licenciamiento futuro para la visualización de Indicadores de Compromiso IOC.

5.2.6. Con la finalidad que el proveedor cumpla con proporcionar una solución de solución de firewall de apliaciones web de acuerdo a las exigencias técnicas requeridas en el presente documento durante el plazo establecido, se aceptará la reposición y/o inclusión de hardware tipo appliance necesario. Para tal efecto, se deberá tener en cuenta las diferentes vigencias tecnológicas publicadas por el fabricante en sus canales de comunicación oficiales.
5.2.7. El proveedor proveerá los materiales tipo cableado, conectores u otros necesarios para el cumplimiento de las actividades tipificadas en el numeral 5.1, en coordinación con la DIRTEL.

5.3. Recursos y facilidades a ser provistos por la Entidad

5.3.1. La Jefatura del Departamento de Administración de Redes y Ciberseguridad brindará las facilidades y accesos para el cumplimiento del servicio requerido.

5.4. Reglamentos sanitarios nacionales

El personal de la empresa adjudicada, que tengan contacto y/o realice actividades de distinta índole (tramite documentario, entrega de material, abastecimiento, brindar servicios o prestaciones, entre otros), dentro de las instalaciones de la Marina de Guerra del Perú, emitirán Declaración Jurada de toma de conocimiento y cumplimiento a los protocolos sanitarios siguientes:

5.4.1. Aislamiento COVID-19.- Procedimiento a responsabilidad de las empresas adjudicadas u otras actividades de distinta índole, por el cual una persona con caso sospechoso, reactivo en la prueba rápida o positivo en la Prueba PCR para COVID-19 será aislado y evacuado en forma inmediata al Centro de Salud para su evaluación correspondiente, debiendo elevar el respectivo informe médico por el postor adjudicado, donde se detallará las indicaciones dadas por la parte médica y su alta médica respectiva.

5.4.2. Distanciamiento Social.- Aumentar el espacio que separa a las personas y reducir la frecuencia de contacto, con el fin de reducir la transmisión de la enfermedad (distancia mínima de DOS (2) metros aproximadamente.

5.4.3. Higiene Respiratoria. - Cubrirse la boca y nariz con UNA (1) tapa boca certificado y aprobado por el MINSA, en todo momento y de manera obligatoria.

5.4.4. Higiene de manos.- Uso de guantes y lavado de manos a menudo con agua y jabón o solución recomendada; de acuerdo a la naturaleza de su visita, de manera obligatoria.

5.4.5. Higiene Ambiental. Mantener la limpieza de los lugares, superficies y movilidades de trabajo, de manera constante y obligatoria.

Asimismo, los postores deberán presentar declaración jurada donde se detalle que el personal a su cargo no presenta sintomatología o haber estado en contacto de personas infectadas con COVID-19, con el propósito de descartar cualquier contagio del personal de la Marina de Guerra del Perú, el postor dará cumplimiento a dispuesto en la Resolución N° 283-2020 MINSA de fecha 13 de mayo del 2020, en lo referente a trabajadores con riesgo y alto riesgo a exposición COVID-19, donde se detalla al personal vulnerable las características de este tipo de personas, las cuales son:

- Mayores de 65 años
- Embarazadas y lactantes
- Enfermos cardiovasculares
- Pacientes con cáncer y/o diabetes mellitus
- Obesos con IMC de 40 a mas
- Asmáticos moderados o graves
- Enfermos respiratorios crónicos
- Enfermos pulmonares crónicos
- Insuficientes renales crónicos en tratamientos con hemodiálisis
- Enfermos o en tratamiento con inmunosupresores
- Otros, bajo responsabilidad del postor adjudicado.

Se aplicará lo establecido según Resolución Ministerial Nro. 265-2020 MINSA de fecha 7 de mayo del 2020, modificada por Resolución Ministerial Nro. 283-2020 MINSA de fecha 13 de mayo del 2020.

5.5. Prestaciones accesorias a la prestación principal

5.5.1. Mantenimiento preventivo

5.5.1.1. Se podrá requerir el mantenimiento preventivo al appliance en forma semestral y en coordinación con la Dirección de Telemática de la Marina.

5.5.2. Soporte técnico

5.5.2.1. Se podrá requerir soporte técnico vía telefónica, correo electrónico o sesión remota, tipo 24x7x365, es decir durante las 24 horas del día, los 7 días de la semana y los 365 días del año, con un tiempo máximo de respuesta de 4 horas. En caso no se pudiera solucionar un incidente a través de los medios antes descritos luego de 48 horas de transcurrido el incidente, el soporte técnico deberá realizarse en forma presencial.

5.5.2.2. Deberá asegurarse el acceso permanente y oportuno a las actualizaciones de seguridad y de rendimiento del equipo appliance firewall de aplicaciones web ofertado, parcial o integral, proporcionado por el fabricante.

5.5.2.3. Se podrá requerir evaluaciones de mejora y/o prevención para el equipo appliance firewall de aplicaciones web, parcial o integral.

5.5.2.4. Se podrá requerir la ejecución de un ASSESSMENT DE SEGURIDAD con una herramienta de pentesting al equipo appliance firewall de aplicaciones web por única vez y en forma coordinada con la Dirección de Telemática de la Marina.

5.5.2.5. Efectuará el escalamiento de soporte a nivel fabricante cuando lo requiera la Dirección de Telemática de la Marina.

5.5.2.6. Deberá proporcionar alternativas de solución para no afectar la continuidad del servicio por un plazo no mayor a 72 horas.

5.5.3. Capacitación

5.5.3.1. Se podrá requerir la capacitación en administración del equipo appliance firewall de aplicaciones web, el cual estará dirigido a un mínimo de TRES (3) técnicos de la División de Ciberseguridad de la DIRTEL, con un tiempo mínimo de duración de 8 horas, a realizarse en las instalaciones de la Entidad, o en forma virtual, dentro de los 3 meses posteriores a la culminación de las actividades tipificadas en el numeral 5.1.

5.5.3.2. El sylabus corresponderá a la versión del equipo appliance firewall de aplicaciones web implementada y será elaborado por el proveedor en coordinación con la DIRTEL.

5.5.3.3. El material a entregar deberá contemplar el detalle de todos los temas a dictarse según el syllabus.

5.5.3.4. Se deberá otorgar constancias de participación para el personal que siga la capacitación.

5.5.4. Garantía

5.5.4.1. El proveedor presentará la garantía de buen funcionamiento será por el mismo periodo de vigencia del licenciamiento. Asimismo, iniciará al mismo tiempo que la vigencia del licenciamiento del software de seguridad implementado por el proveedor.

5.5.4.2. La garantía de buen funcionamiento comprende que la solución ofertada cumpla con todos los requerimientos tipificados en el presente documento.

5.6. Lugar y plazo de la prestación

5.6.1. Lugar

La prestación del servicio será en la Dirección de Telemática de la Marina, cito en Av. La Marina Cdra. 36 S/N, dentro de la Estación Naval La Perla.

5.6.2. Plazo

5.6.2.1. El plazo para la configuración del servicio del periodo comprendido entre los años 2021 - 2022, será de 50 días calendario, contabilizados a partir del día siguiente de la firma del contrato.
5.6.2.2. La configuración del servicio del periodo comprendido entre los años 2022 – 2023 y 2023 - 2024, será de máximo 10 días calendarios antes de la caducidad de la licencia vigente.
5.6.2.3. El plazo de ejecución del servicio es de 1,095 días calendarios, dividido en tres periodos de 365 días calendarios entre los años 2021 y 2024, los mismos que corresponden a la duración del licenciamiento anual a ser expedidas.

5.7. Confidencialidad

El POSTOR deberá firmar el Acta de Confidencialidad proporcionado por la Dirección de Telemática de la Marina, para el desarrollo de los trabajos de soporte técnico y otros que se realicen sobre los sistemas informáticos de la institución, el cual se realizará a la firma del contrato.

El acuerdo de confidencialidad formará parte del contrato a fin de permitir y resguardar la información clasificada de la Institución, pudiéndose limitar el acceso de profesionales que puedan afectar a la seguridad de la Institución.

5.8. Medidas de control durante la ejecución contractual

5.8.1. Designación de responsabilidades

5.8.1.1. Áreas que coordinarán con el proveedor: La Jefatura del Departamento de Administración de Redes y Ciberseguridad y la División de Ciberseguridad.
5.8.1.2. Área responsable de las medidas de control: La Jefatura del Departamento de Administración de Redes y Ciberseguridad.
5.8.1.3. Área que brindará la conformidad: La Jefatura de la División de Ciberseguridad.

5.8.2. Medidas de control

5.8.2.1. Supervisará que el proveedor cumpla con todo lo requerido en el presente documento.
5.8.2.2. Verificará la correcta confección del Acta de Conformidad.

5.8.3. Conformidad

Se elaborarán Actas de Conformidad en forma anual, posterior a la configuración del servicio de licenciamiento requerido, debiendo contener los siguientes documentos:

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

5.8.3.1. Screenshot del portal oficial del fabricante donde figuren las claves u otros indicadores que permita validar la licencia proporcionada.
5.8.3.2. Informe elaborado por el proveedor donde acredite el cumplimiento de lo tipificado en el numeral 5.1.
5.8.3.3. Declaración jurada del proveedor en el cual se compromete a brindar el mantenimiento preventivo, soporte técnico, capacitación y garantía de buen funcionamiento, de acuerdo a lo tipificado del numeral 5.5.1 al numeral 5.5.4. En dicho documento el proveedor deberá indicar los teléfonos y correos electrónicos para contacto.

5.9. Forma de pago

El pago se realizará en TRES (03) armadas, previa presentación del acta de conformidad detallada en el numeral 5.9.3, de acuerdo a lo siguiente:

5.9.1. El primer pago se efectuará en el año 2021 y corresponderá al 33.33% del monto contractual.
5.9.2. El segundo pago se efectuará en el año 2022 y corresponderá al 33.33% del monto contractual.
5.9.3. El segundo pago se efectuará en el año 2023 y corresponderá al 33.34% del monto contractual.

ÍTEM N°3
SERVICIO DE LICENCIAMIENTO PARA EL SISTEMA DE SEGURIDAD INFORMÁTICA DE NAVEGACIÓN PROXY WEB Y FILTRADO DE CONTENIDO

I. TÉRMINOS DE REFERENCIA

1. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de Licenciamiento para el Sistema de Seguridad Informática de Navegación Proxy Web y Filtrado de contenido.

2. FINALIDAD PÚBLICA

La MARINA DE GUERRA DEL PERÚ, requiere contar con el servicio de Licenciamiento para el Sistema de Seguridad Informática de Navegación Proxy Web y Filtrado de Contenido, con la finalidad de asegurar el perímetro interno y externo de la WAN Naval, así como efectuar el monitoreo de la red informática institucional.

3. ANTECEDENTES

La Entidad, dentro de su estrategia de seguridad de la información institucional, posee un conjunto de soluciones de seguridad informática que permiten proteger la información que se encuentra almacenada en los diferentes equipos informáticos, estaciones de trabajo y servidores.

En tal sentido, el presente proceso se enfoca en renovar y continuar con la seguridad que se obtiene al filtrar el tráfico web de los usuarios y agentes automatizados a través un flujo centralizado por un proxy web.

4. OBJETIVO DE LA CONTRATACIÓN

Mantener el nivel de seguridad de la información de la Entidad a través de la renovación del licenciamiento de la solución de navegación proxy web y filtro de contenido en alta disponibilidad.

5. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

5.1. Actividades

Las siguientes actividades serán realizadas en forma anual, en cumplimiento a la contratación del servicio y en coordinación con la Dirección de Telemática de la Marina, en adelante DIRTEL:

5.1.1. Generación de las licencias correspondientes a la solución de navegación proxy web y filtro de contenido y remisión a la DIRTEL.
5.1.2. Instalación y/o configuración de la solución propuesta de ser requerido.
5.1.3. Instalación de la nueva licencia en la solución.
5.1.4. Revisión y/u optimización integral de la solución.

5.2. Recursos a ser provistos por el proveedor

5.2.1. TRES (3) licenciamientos anuales (vigencia de 365 días cada uno) de la solución de navegación proxy web y filtro de contenido para TRES MIL (3,000) usuarios concurrentes y alta disponibilidad a nombre de la Marina de Guerra del Perú.
5.2.2. La solución de navegación proxy web y filtro de contenido presentará alta disponibilidad tipo cluster.
5.2.3. Las funcionalidades básicas de la solución de navegación proxy web y filtro de contenido serán las siguientes:

5.2.3.1. El licenciamiento debe soportar proxy para HTTP, HTTPS, FTP, FTP sobre HTTP, SOCKS.
5.2.3.2. El licenciamiento debe permitir tecnología de web caching para proveer mejoras adicionales en el desempeño de la red mediante el uso de contenido que sea reusable y de almacenamiento local. Se espera que la solución mejore los tiempos de respuesta del acceso a internet y mejore el uso del ancho de banda del enlace de internet.
5.2.3.3. El licenciamiento deberá tener la facultad de instalarse en hardware de servidores abiertos y soportar virtualización tanto en sistemas como Hyper-V o VMWare. En este caso, no deberá tener licenciamiento aparte y podrá instalarse N veces como parte del licenciamiento entregado, sea en formato virtual o en software
5.2.3.4. El licenciamiento deberá soportar poder instalarse en appliance físicos o appliances virtuales, en la nube y en modo hibrido, en cualquier momento que sea requerido por la organización, dentro del periodo de contrato.
5.2.3.5. Deberá soportar licenciamiento a futuro para la integración con tecnología de tipo "Remote Browser Isolation (RBI)", que permita aislar la navegación web del usuario final en contenedores virtuales, protegiéndolos de sitios riesgosos, sitios web desconocidos, así como procesar y permitir acceder a las URL incorporadas en correos electrónicos (phishing) en modo de solo lectura, creando una experiencia segura y sin complicaciones para el usuario final.
5.2.3.6. Deberá soportar licenciamiento a futuro para un proceso de saneamiento de datos o CDR (Desarmado y Recuperación de Contenido) completamente integrada, para limpiar archivos entrantes de contenido potencialmente malicioso antes de entregarlos al usuario final.
5.2.3.7. Deberá soportar licenciamiento a futuro para la integración con tecnología de CASB (Cloud Access Security Broker) del mismo fabricante, para poder controlar el acceso (Login, Logout) y otras actividades (Upload, Download, View, Modify, Create, Delete, etc) hacia dichas aplicaciones autorizadas (por ejemplo, O365, GSuite, etc.), en tiempo Real. Dicha integración debe ser transparente para el usuario final y No debe requerir instalar algún otro agente adicional, al que se incluya en la propuesta de Seguridad Web para la navegación de usuarios remotos.

5.2.4. Las funcionalidades específicas de la solución de navegación proxy web y filtro de contenidos relacionados a la distribución e instalación serán los siguientes:

5.2.4.1. El licenciamiento debe permitir diversos modos de implementación. Se espera que la solución pueda configurarse como proxy explícito y como proxy transparente.
5.2.4.2. El modo de operación proxy transparente debe incluir: Soporte para usar WCCP (Web Cache Content Protocol) y PBR (Policy Based Routing).
5.2.4.3. El modo de operación proxy explicito debe incluir lo siguiente: configuración manual de browser y/o soporte para auto configuración del proxy mediante el uso de PAC, WPAC y políticas de Active Directory.
5.2.4.4. La solución debe soportar configuración de proxy en cadena para poder integrarse con arquitecturas de proxies existentes.

5.2.5. Las funcionalidades específicas de la solución de navegación proxy web y filtro de contenido para clustering y alta disponibilidad serán los siguientes:

5.2.5.1. El licenciamiento debe tener la capacidad de ser implementada en modo clúster, con soporte para políticas y configuración unificada para todos los componentes del arreglo lógico que hacen parte del cluster. Debe soportar configuraciones Activo-Activo y Activo-Pasivo para poseer alta disponibilidad para el servicio de acceso web con el uso de failover que puede involucrar a 2 o más nodos.

5.2.5.2. El licenciamiento debe permitir integrarse con componentes de filtrado en software que podrán instalarse en sistemas operativos Microsoft Windows Server 2012 R2, 2016, 2019 Standard Edition de 64 bits, Linux Red Hat 7.6, 7.7 o CentOS en la misma versión y poder compartir las políticas de seguridad indistintamente en donde estén los componentes distribuidos

5.2.5.3. El licenciamiento debe permitir hacer uso de las siguientes tecnologías para alta disponibilidad: Virtual IP, DNS Round Robin,y clustering administrado.

5.2.5.4. El licenciamiento debe permitir WCCP (Web Cache Content Protocol) para ser usado en conjunto con un router para proveer alta disponibilidad, adicionalmente debe soportar el uso de balanceadores de carga para resiliencia y escalabilidad.

5.2.5.5. El licenciamiento podrá instalarse bajo el sistema operativo Linux RedHat/Centos 7.6 o 7.7. El comportamiento del proxy bajo este sistema operativo debe tener el mismo comportamiento y habilidad que su símil en Appliance propietario. Esto no deberá tener costo adicionalCompatibilidad con Sistemas Operativos Windows Server 2008 R2, 2012, 2016 y superior (64 bits).

5.2.6. Las funcionalidades específicas de la solución de navegación proxy web y filtro de contenido para los métodos de autenticación de proxy serán los siguientes:

5.2.6.1. El licenciamiento deberá proveer autenticación selectiva utilizando diferentes tipos de autenticación que podrán ser usados de manera simultánea en un mismo ambiente. Los administradores podrán especificar ciertos usuarios para ser autenticados de manera transparente (no login) mientras que otros usuarios deberán autenticarse de manera manual (login required) de forma tal que se puedan usar y aplicar políticas apropiadas en ambientes donde se tengan PC compartidos, PC para uso del público y PC para uso de empleados corporativos

5.2.6.2. El Proxy Web debe soportar los siguientes métodos de autenticación: Active Directory, LDAP, RADIUS, Integrated Windows Authentication (IWA)

5.2.7. Las funcionalidades específicas de la solución de navegación proxy web y filtro de contenido para la inspección y desencriptación de protocolo SSL serán los siguientes:

5.2.7.1. Debe usar tecnología que permita desencriptación on-box de tráfico HTTPS para inspección profunda de dicho tráfico y aplicación de políticas en el mismo appliance.

5.2.7.2. Debe permitir la administración de certificados digitales con el uso de una consola web desde donde también se debe permitir el uso de políticas globales y generación de reportes con el fin de disminuir las tareas administrativas.

5.2.7.3. La solución debe prevenir ataques encriptados mediante la capacidad de realizar desencriptación de SSL en el Gateway. Una vez abierto el túnel, debe aplicar análisis de motor antivirus basado en la misma caja, análisis de contenido en tiempo real en la misma caja y detección de aplicaciones mediante fingerprint en la misma caja. No se aceptarán soluciones que utilicen mecanismos mediante ICAP o Secure ICAP para realizar dichas funciones

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

5.2.7.4. Debe soportar licenciamiento futuro para activar DLP en el canal de WEB, deberá contar con más de 1,500 plantillas de políticas de prevención de fuga de datos precargadas (PCI, PII, entre otros), que apliquen por países (Ecuador, Perú, Bolivia, Colombia, Chile, Argentina, etc.) y por vertical de Industria, como: Educación, Energía e Infraestructura, Entretenimiento, Financieras y Banca, Gobierno, Hardware, Cuidado de Salud, Seguros, Manufacturas, Retail, Software, Telco, Transporte entre otros.

5.2.7.5. Debe soportar licenciamiento futuro para la funcionalidad OCR (Optical Character Recognition) para el canal de comunicación WEB

5.2.8. Las funcionalidades específicas de la solución de navegación proxy web y filtro de contenido para la clasificación dinámica de contenido en tiempo real serán los siguientes:

5.2.8.1. El licenciamiento debe proveer clasificación en tiempo real en más de 120 categorías de filtro de contenido (Viajes, deportes, contenido adulto, etc) mediante la extracción de elementos (lenguaje natural, palabras clave, colores, fuentes, títulos, fondos) y clasificar este contenido en tiempo real usando algoritmos propietarios de la solución y base de datos de categorías propietaria del fabricante de la solución. Todo este análisis debe ser realizado on-box (en la misma caja) sin requerir consultas de reputación en la nube o técnicas de categorización dinámica en la nube.

5.2.8.2. Debe proveer análisis de seguridad en tiempo real con el fin de identificar y evitar que amenazas como spyware, phishing, malware, entre otros, lleguen a comprometer los usuarios del servicio de navegación, la solución debe contar con la capacidad de extraer componentes activos (scripts, exploits, código binario, imágenes, entre otros) que se encuentren dentro del contenido web que pueda activar cualquier actividad malintencionada. Este análisis debe ser realizado on-box(en la misma caja). No se aceptarán soluciones que requieran Appliance adicionales para dichos trabajos ni que requieran ICAP o Secure ICAP para tal tarea o que requieran conectividad a servicios en la nube para dichas tareas

5.2.9. Las funcionalidades específicas de la solución de navegación proxy web y filtro de contenido para la funcionalidad de filtrado web serán los siguientes:

5.2.9.1. Debe tener 120 categorías diferentes dentro de una base de datos propietaria del fabricante de la solución. No se aceptarán soluciones de filtrado que no sean del propio fabricante. Debe presentar documentación oficial del fabricante en donde se listen las categorías ofertadas

5.2.9.2. Debe tener 120 protocolos dentro de la base de datos de protocolos. Estos protocolos podrán ser detectados ya sea tunelizados, es decir, a través del puerto 80 o 443 o de forma nativa, es decir, protocolos que salgan de forma directa hacia a Internet sin considerar el uso del proxy mediante la misma consola y sin necesidad de software off box para detectar protocolos.

5.2.9.3. Debe realizar actualizaciones diarias, con descargas incrementales con opción de actualizaciones dinámicas y desatendidas.

5.2.9.4. Debe tener categorías separadas para sitios web que afectan el tiempo de productividad de los empleados y sitios que afecta el ancho de banda del acceso a internet

5.2.9.5. Debe tener categoría separada para Seguridad: Allí debe estar contenidos sitios web que presentan amenazas como:

a. Bot networks
b. Keyloggers
c. Malicious Embedded iFrame
d. Malicious Embedded Link
e. Malicious Web Sites
f. Phishing and Others Frauds

g. Potencially Unwanted Software
h. Spyware
i. Suspicious Embedded Link

5.2.9.6. No se consideran soluciones que no cuenten con estas categorías mínimas exigidas.

5.2.9.7. Debe tener los siguientes controles para el manejo de Facebook:
a. Facebook Friends
b. Facebook Photo Upload
c. Facebook Mail
d. Facebook Events
e. Facebook Apps
f. Facebook Chat
g. Facebook Questions
h. Facebook Video Upload
i. Facebook Groups
j. Facebook Games

5.2.9.8. Se exige el listado de los controles de Facebook presentados por el producto que debe cumplir mínimamente con los solicitados en este punto. Incluir listado con un documento del propio fabricante.

5.2.9.9. Debe tener los siguientes controles para el manejo de Linkedin:
a. LinkedIn Connections
b. LinkedIn Jobs
c. LinkedIn Mail
d. LinkedIn Updates

5.2.9.10. Se exige que la solución cumpla como mínimo con estos controles. Debe presentar un documento del propio fabricante

5.2.9.11. Debe tener los siguientes controles para el manejo de Twitter:
a. Twitter Follow
b. Twitter Mail
c. Twitter Posting

5.2.9.12. Se exige que la solución cumpla como mínimo con estos controles. Debe presentar un documento del propio fabricante

5.2.9.13. Debe tener los siguientes controles para YouTube
a. YouTube Commenting
b. Youtube Sharing
c. Youtube video Upload

5.2.9.14. Se exige que la solución cumpla como mínimo con estos controles. Debe presentar un documento del propio fabricante

5.2.9.15. Deberá garantizar que nuevas páginas cuyo contenido represente riesgos a la seguridad sean agregadas automáticamente a la lista de URL's máximo cinco minutos después de haber sido descubiertas por el fabricante de la solución, durante el transcurso del día y de manera automatizada aparte de la clasificación que ya realiza en forma dinámica con motores analíticos locales

5.2.9.16. Deberá permitir la reclasificación manual de cualquier página Web según las necesidades de la empresa, bien como permitir que ciertas páginas puedan ser accedidas a cualquier momento, aunque pertenezcan a categorías bloqueadas

5.2.9.17. Deberá permitir la definición de políticas por IP, rangos de IP's, usuarios y grupos de los siguientes servicios de directorio para HTTP(S)/FTP sobre HTTP:
a. Dominios del Microsoft Windows NT (NTLM)
b. Dominios del Microsoft Active Directory
c. Directorios LDAP

5.2.9.18. Deberá permitir la definición de una política general que aplique a aquellos usuarios que no tengan una política especifica asignada

5.2.9.19. Deberá enviar una alerta administrativa por e-mail, popup o SNMP caso haya un número (configurable) accesos a páginas de las categorías deseadas durante el día.

5.2.9.20. Debe permitir excepciones basadas en las cabeceras de referer de http (http referer header). Por ejemplo, deberá bloquear acceso a Youtube a los empleados, salvo cuando los videos estén vinculados a la intranet de la empresa.

5.2.9.21. Debe bloquear aplicaciones para Windows maliciosas mediante el uso de Reconocimiento de Aplicaciones, Detección Avanzada de Aplicaciones y Análisis de Seguridad en Tiempo Real. Este debe ser un motor de seguridad adicional que permita identificar ciertos archivos binarios como herramientas de hacking renombradas entre otros.

5.2.9.22. El licenciamiento debe tener la capacidad de entender los sitios web, contenido web, aplicaciones y malware, más allá de la reputación misma del sitio considerando el uso y el contexto del mismo en Internet de manera que se logre un análisis del riesgo del sitio en tiempo real. Aun si un sitio confiable que goce de buena reputación es comprometido la solución deberá poder prevenir la amenaza.

5.2.10. Las funcionalidades específicas de la solución de navegación proxy web y filtro de contenido para la administración de protocolos de red serán los siguientes:

5.2.10.1. Debe manejar y permitir controlar otros protocolos diferentes a http, https, ftp (IM, P2P, streaming media, entre otros) tunelizados y no tunelizados, a través de un puerto tipo SPAN.

5.2.10.2. Debe actualizar su lista de protocolos de manera dinámica sin necesidad de subir de versión o cambiar firmware.

5.2.10.3. La solución debe tener la capacidad de aplicar políticas basadas en 120 protocolos mínimamente.

5.2.10.4. La solución no deberá contar con una plataforma o consola adicional para gestionar los protocolos. Se requiere que los informes sean consolidados y que puedan ofrecen tanto la información de protocolos y de URL.

5.2.11. Las funcionalidades específicas de la solución de navegación proxy web y filtro de contenido para la administración del ancho de banda serán los siguientes:

5.2.11.1. El licenciamiento debe brindar la capacidad de asignar umbrales de ancho de banda para varias URL, categorías de URL, protocolos y categorías de protocolos.

5.2.11.2. Debe permitir aplicar políticas de ancho de banda para usuarios y grupos.

5.2.11.3. Debe permitir aplicar políticas de ancho de banda por protocolos.

5.2.11.4. Debe permitir aplicar políticas de ancho de banda para usuarios y grupos.

5.2.11.5. Debe permitir aplicar políticas de ancho de banda por protocolos

5.2.11.6. Los empleados deben ser notificados cuando sobrepasen los límites de ancho de banda configurados en las políticas.

5.2.12. Las funcionalidades específicas de la solución de navegación proxy web y filtro de contenido para la consola de administración y reportes serán los siguientes:

5.2.12.1. Debe proveer la capacidad de distribuir las políticas desde una ubicación central hacia múltiples appliances distribuidos por toda la organización.

5.2.12.2. Debe tener una consola Web para gestión, administración y generación de reportes.

5.2.12.3. El licenciamiento debe soportar múltiples clases de administradores, como mínimo debe tener los siguientes: Super Administrador, Administrador Delgado, Administrador Remoto. Adicionalmente debe permitir la administración delegada de políticas y reportes.

5.2.12.4. Las actividades ejecutadas por los administradores deben ser auditables y dicha auditoria debe ser parte integral de la solución

5.2.12.5. Debe tener la capacidad de recategorizar websites de manera automática o por requerimientos de la organización.
5.2.12.6. El licenciamiento debe permitir reportes tipo drill down que se puedan generar y consultar desde la consola web. Estos reportes deben proveer datos históricos y deben tener al menos 80 plantillas predefinidas que puedan ser utilizadas.
5.2.12.7. El licenciamiento debe proveer información del desempeño del cache y de los recursos en uso.
5.2.12.8. Debe tener la capacidad de delegar la generación de reportes y debe permitir que el delegatario tenga capacidad de generar los reportes para un grupo específico de usuarios.
5.2.12.9. Deberá poseer servicio de almacenamiento de registros de actividades, el cual guarde dichos registros en una base de datos SQL Server 2008, SQL 2016 o 2017. El sistema de reportería no debe estar limitado a la cantidad de resultados de una consola y no debe tener licenciamiento adicional.
5.2.12.10. Deberá poseer mecanismo de mantenimiento de la base de datos, el cual deberá permitir el borrado o archivado de registros anteriores a cierta fecha, o bien mover registros anteriores a cierta fecha hacia una base de logs historial.
5.2.12.11. La interfaz de generación de reportes deberá permitir exportarse los reportes generados para mínimo los siguientes formatos:
a. Microsoft Excell
b. Acrobat PDF
c. HTML
5.2.12.12. La interfaz de generación de reportes deberá permitir la programación de múltiples tareas de generación de reportes predeterminados, en horarios y días de la semana predefinidos, y deberá:
5.2.12.13. Enviar los reportes generados por correo electrónico hacia los recipientes deseados
5.2.12.14. La interfaz de acceso directo a los registros de log deberá permitir la personalización de los reportes generados
5.2.12.15. Se podrá generar reportes de Riesgos de Seguridad presentes, como que usuarios/IP han sido atacados con Spyware, Phising, Adware, Keyloggers, etc
5.2.12.16. Se generarán reportes en función de cuanto ancho de banda consumen estas clases de riegos (bytes Enviados/Recibidos/Total).
5.2.12.17. Se podrá configurar que se manden alertas en tiempo real, a correo electrónico o en pantalla, sobre estos riegos, a detalle, con información sobre Usuario/IP, Categoría accedida, Sitio/URL, IP del Sitio, la disposición (si fue bloqueada o permitida de acuerdo a las políticas), hora y fecha.

5.2.13. Con la finalidad que el proveedor cumpla con proporcionar una solución de navegación proxy web y filtro de contenido de acuerdo a las exigencias técnicas requeridas en el presente documento durante el plazo establecido, se aceptará la reposición y/o inclusión de hardware tipo appliance. Para tal efecto, se deberá tener en cuenta las diferentes vigencias tecnológicas publicadas por los fabricantes en sus canales de comunicación oficiales.
5.2.14. El proveedor proveerá los materiales tipo cableado, conectores u otros necesarios para el cumplimiento de las actividades tipificadas en el numeral 5.1, en coordinación con la DIRTEL.

5.3. Recursos y facilidades a ser provistos por la Entidad

5.3.1. La Jefatura del Departamento de Administración de Redes y Ciberseguridad brindará las facilidades y accesos para el cumplimiento del servicio requerido.
5.3.2. La Entidad brindará una máquina virtual para la instalación de la consola de administración en coordinación con la DIRTEL. Dicha máquina virtual deberá poseer las siguientes características: 8 vCPU, 24GB de RAM y 500GB de disco.

MINISTERIO DE DEFE... – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

5.4. Reglamentos sanitarios nacionales

El personal de la empresa adjudicada, que tengan contacto y/o realice actividades de distinta índole (tramite documentario, entrega de material, abastecimiento, brindar servicios o prestaciones, entre otros), dentro de las instalaciones de la Marina de Guerra del Perú, emitirán Declaración Jurada de toma de conocimiento y cumplimiento a los protocolos sanitarios siguientes:

5.4.1. Aislamiento COVID-19.- Procedimiento a responsabilidad de las empresas adjudicadas u otras actividades de distinta índole, por el cual una persona con caso sospechoso, reactivo en la prueba rápida o positivo en la Prueba PCR para COVID-19 será aislado y evacuado en forma inmediata al Centro de Salud para su evaluación correspondiente, debiendo elevar el respectivo informe médico por el postor adjudicado, donde se detallará las indicaciones dadas por la parte médica y su alta médica respectiva.
5.4.2. Distanciamiento Social.- Aumentar el espacio que separa a las personas y reducir la frecuencia de contacto, con el fin de reducir la transmisión de la enfermedad (distancia mínima de DOS (2) metros aproximadamente.
5.4.3. Higiene Respiratoria. - Cubrirse la boca y nariz con UNA (1) tapa boca certificado y aprobado por el MINSA, en todo momento y de manera obligatoria.
5.4.4. Higiene de manos.- Uso de guantes y lavado de manos a menudo con agua y jabón o solución recomendada; de acuerdo a la naturaleza de su visita, de manera obligatoria.
5.4.5. Higiene Ambiental. Mantener la limpieza de los lugares, superficies y movilidades de trabajo, de manera constante y obligatoria.

Asimismo, los postores deberán presentar declaración jurada donde se detalle que el personal a su cargo no presenta sintomatología o haber estado en contacto de personas infectadas con COVID-19, con el propósito de descartar cualquier contagio del personal de la Marina de Guerra del Perú, el postor dará cumplimiento a dispuesto en la Resolución N° 283-2020 MINSA de fecha 13 de mayo del 2020, en lo referente a trabajadores con riesgo y alto riesgo a exposición COVID-19, donde se detalla al personal vulnerable las características de este tipo de personas, las cuales son:

- Mayores de 65 años
- Embarazadas y lactantes
- Enfermos cardiovasculares
- Pacientes con cáncer y/o diabetes mellitus
- Obesos con IMC de 40 a mas
- Asmáticos moderados o graves
- Enfermos respiratorios crónicos
- Enfermos pulmonares crónicos
- Insuficientes renales crónicos en tratamientos con hemodiálisis
- Enfermos o en tratamiento con inmunosupresores
- Otros, bajo responsabilidad del postor adjudicado.

Se aplicará lo establecido según Resolución Ministerial Nro. 265-2020 MINSA de fecha 7 de mayo del 2020, modificada por Resolución Ministerial Nro. 283-2020 MINSA de fecha 13 de mayo del 2020.

5.5. Prestaciones accesorias a la prestación principal

5.5.1. Mantenimiento preventivo

5.5.1.1. Se efectuará el mantenimiento preventivo de la solución de navegación proxy web y filtro de contenido en forma semestral y en coordinación con la Dirección de Telemática de la Marina.

5.5.2. Soporte técnico

5.5.2.1. Se efectuará el soporte técnico vía telefónica, correo electrónico o sesión remota, tipo 24x7x365, es decir durante las 24 horas del día, los 7 días de la semana y los 365 días del año, con un tiempo máximo de respuesta de 4 horas. En caso no se pudiera solucionar un incidente a través de los medios antes descritos luego de 48 horas de transcurrido el incidente, el soporte técnico deberá realizarse en forma presencial.
5.5.2.2. Deberá asegurarse el acceso permanente y oportuno a las actualizaciones de seguridad y de rendimiento de la solución de navegación proxy web y filtro de contenido ofertado, parcial o integral, proporcionado por el fabricante.
5.5.2.3. Se efectuará evaluaciones de mejora y/o prevención para la solución de navegación proxy web y filtro de contenido, parcial o integral.
5.5.2.4. Se efectuará la ejecución de un ASSESSMENT DE SEGURIDAD con una herramienta de pentesting a la solución de navegación proxy web y filtro de contenido por única vez y en forma coordinada con la Dirección de Telemática de la Marina.
5.5.2.5. Efectuará el escalamiento de soporte a nivel fabricante cuando lo requiera la Dirección de Telemática de la Marina.
5.5.2.6. Deberá proporcionar alternativas de solución para no afectar la continuidad del servicio por un plazo no mayor a 72 horas.

5.5.3. Capacitación

5.5.3.1. Se efectuará en administración de la solución de navegación proxy web y filtro de contenido, el cual estará dirigido a un mínimo de TRES (3) técnicos de la División de Ciberseguridad de la DIRTEL, con un tiempo mínimo de duración de 8 horas, a realizarse en las instalaciones de la Entidad, o en forma virtual, dentro de los 3 meses posteriores a la culminación de las actividades tipificadas en el numeral 5.1.
5.5.3.2. El sylabus corresponderá a la versión de la solución de seguridad informática tipo antivirus implementada y será elaborado por el proveedor en coordinación con la DIRTEL.
5.5.3.3. El material a entregar deberá contemplar el detalle de todos los temas a dictarse según el sylabus.
5.5.3.4. Se deberá otorgar constancias de participación para el personal que siga la capacitación.

5.5.4. Garantía

5.5.4.1. El proveedor presentará la garantía de buen funcionamiento será por el mismo periodo de vigencia del licenciamiento. Asimismo, iniciará al mismo tiempo que la vigencia del licenciamiento del software de seguridad implementado por el proveedor.
5.5.4.2. La garantía de buen funcionamiento comprende que la solución ofertada cumpla con todos los requerimientos tipificados en el presente documento.

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

5.6. Lugar y plazo de la prestación

5.6.1. Lugar

La prestación del servicio será en la Dirección de Telemática de la Marina, cito en Av. La Marina Cdra. 36 S/N, dentro de la Estación Naval La Perla.

5.6.2. Plazo

5.6.2.1. El plazo para la configuración del servicio del periodo comprendido entre los años 2021 - 2022, será de 50 días calendario, contabilizados a partir del día siguiente de la firma del contrato.
5.6.2.2. La configuración del servicio del periodo comprendido entre los años 2022 – 2023 y 2023 - 2024, será de máximo 10 días calendarios antes de la caducidad de la licencia vigente.
5.6.2.3. El plazo de ejecución del servicio es de 1,095 días calendarios, dividido en tres periodos de 365 días calendarios entre los años 2021 y 2024, los mismos que corresponden a la duración del licenciamiento anual a ser expedidas.

5.7. Confidencialidad

El POSTOR deberá firmar el Acta de Confidencialidad proporcionado por la Dirección de Telemática de la Marina, para el desarrollo de los trabajos de soporte técnico y otros que se realicen sobre los sistemas informáticos de la Institución, el cual se realizará a la firma del contrato.

El acuerdo de confidencialidad formará parte del contrato a fin de permitir y resguardar la información clasificada de la Institución, pudiéndose limitar el acceso de profesionales que puedan afectar a la seguridad de la Institución.

5.8. Medidas de control durante la ejecución contractual

5.8.1. Designación de responsabilidades

5.8.1.1. Áreas que coordinarán con el proveedor: La Jefatura del Departamento de Administración de Redes y Ciberseguridad y la División de Ciberseguridad.
5.8.1.2. Área responsable de las medidas de control: La Jefatura del Departamento de Administración de Redes y Ciberseguridad.
5.8.1.3. Área que brindará la conformidad: La Jefatura de la División de Ciberseguridad.

5.8.2. Medidas de control

5.8.2.1. Supervisará que el proveedor cumpla con todo lo requerido en el presente documento.
5.8.2.2. Verificará la correcta confección del Acta de Conformidad.

5.8.3. Conformidad

Se elaborarán Actas de Conformidad en forma anual, posterior a la configuración del servicio de licenciamiento requerido, debiendo contener los siguientes documentos:

5.8.3.1. Screenshot del portal oficial del fabricante donde figuren las claves u otros indicadores que permita validar la licencia proporcionada.
5.8.3.2. Informe elaborado por el proveedor donde acredite el cumplimiento de lo tipificado en el numeral 5.1.
5.8.3.3. Declaración jurada del proveedor en el cual se compromete a brindar el mantenimiento preventivo, soporte técnico, capacitación y garantía de buen funcionamiento, de acuerdo a lo tipificado del numeral 5.5.1 al numeral 5.5.4. En dicho documento el proveedor deberá indicar los teléfonos y correos electrónicos para contacto.

5.9. Forma de pago

El pago se realizará en TRES (03) armadas, previa presentación del acta de conformidad detallada en el numeral 5.9.3, de acuerdo a lo siguiente:

5.9.1. El primer pago se efectuará en el año 2021 y corresponderá al 33.33% del monto contractual.
5.9.2. El segundo pago se efectuará en el año 2022 y corresponderá al 33.33% del monto contractual.
5.9.3. El segundo pago se efectuará en el año 2023 y corresponderá al 33.34% del monto contractual.

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

ÍTEM N°4
SERVICIO DE LICENCIAMIENTO PARA EL SISTEMA DE SEGURIDAD INFORMÁTICA ANTIVIRUS

I. TÉRMINOS DE REFERENCIA

1. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de licenciamiento para el Sistema de Seguridad informática Antivirus

2. FINALIDAD PÚBLICA

El presente requerimiento tiene por finalidad que la Institución disponga de una solución Antivirus y Detección y Respuesta de Amenazas que proteja de forma segura, confiable y sólida los equipos informáticos.

3. ANTECEDENTES

La Entidad, dentro de su estrategia de seguridad de la información institucional, posee un conjunto de soluciones de seguridad informática que permiten proteger la información que se encuentra almacenada en los diferentes equipos informáticos, estaciones de trabajo y servidores.

En tal sentido, el presente proceso se enfoca en renovar y continuar con la seguridad que se brinda a los equipos informáticos en forma individualizada a través de agentes antivirus.

4. OBJETIVO DE LA CONTRATACIÓN

Mantener el nivel de seguridad de la información de la Entidad a través de la renovación del licenciamiento de la solución de seguridad informática tipo antivirus para SEIS MIL (6,000) equipos informáticos, entre estaciones de trabajo y servidores, cuyos agentes podrán ser administrados en forma centralizada.

5. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

5.1. Actividades

Las siguientes actividades serán realizadas en forma anual, en cumplimiento a la contratación del servicio y en coordinación con la Dirección de Telemática de la Marina, en adelante DIRTEL:

5.1.1. Generación de las licencias correspondientes a la solución de seguridad informática tipo antivirus y remisión a la DIRTEL.
5.1.2. Instalación de la nueva licencia en la consola de gestión.
5.1.3. Configuración o reinstalación, de ser el caso, de la consola de gestión.
5.1.4. Despliegue de los agentes antivirus, en caso de ser necesario.
5.1.5. Revisión y/u optimización de la solución de seguridad informática tipo antivirus en forma integral.

5.2. Recursos a ser provistos por el proveedor

5.2.1. TRES (3) licenciamientos anuales (vigencia de 365 días cada uno) de la solución de seguridad informática tipo antivirus con al menos SEIS MIL (6,000) a nombre de la Marina de Guerra del Perú.

5.2.2. Las funcionalidades básicas de la solución de seguridad informática tipo antivirus serán las siguientes:

5.2.2.1. La solución deberá contar con certificación AVTest (www.av-test.org) con calificación igual al valor de dieciocho (18) del total de las 03 pruebas o el valor de seis (6) para cada una de las pruebas realizadas, como son "Protección", "Rendimiento" y "Usabilidad". La calificación indicada debe incluir fecha de emisión, la que no debe ser mayor a un (1) año de antigüedad y debe corresponderse con la versión de software incluida en la Oferta.

5.2.2.2. Se debe acceder a la consola de gestión centralizada vía WEB (HTTPS), MMC.

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

5.2.2.4. Capacidad de instalar remotamente la solución en los equipos informáticos Windows, a través de la administración compartida, login script y/o GPO de Active Directory;

5.2.2.5. Capacidad de gestionar estaciones de trabajo y servidores de archivos (tanto Windows como Linux y Mac) protegidos por la solución;

5.2.2.6. Capacidad de gestionar smartphones y tablets (tanto Android y iOS) protegidos por la solución.

5.2.2.7. Capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto;

5.2.2.8. Capacidad de actualizar los paquetes de instalación con las últimas vacunas, para que cuando el paquete sea utilizado en una instalación ya contenga las últimas vacunas lanzadas;

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

5.2.2.10. Capacidad de monitorear grupos de trabajos ya existentes y cualquier grupo de trabajo que sea creado en la red, a fin de encontrar equipos informáticos nuevos para ser agregadas a la protección;

5.2.2.11. Capacidad de, al detectar máquinas nuevas en el Directorio Activo, subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antimalware instalado. En caso de no tenerlo, debe instalar el agente antivirus automáticamente;

5.2.2.12. Capacidad de agrupamiento de máquinas por características comunes entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antimalware instalado, agrupar todos los equipos informáticos que no recibieron actualización en los últimos 2 días, etc.;

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

5.2.2.14. Compatibilidad con Windows Failover clustering u otra solución de alta disponibilidad.

5.2.2.15. Capacidad de importar la estructura del Directorio Activo para encontrar equipos informáticos;

5.2.2.16. Debe proporcionar las siguientes informaciones de los equipos informáticos:

a. Si el antimalware está instalado;
b. Si el antimalware ha iniciado;
c. Si el antimalware está actualizado;
d. Minutos/horas desde la última conexión de la máquina con el servidor administrativo

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

e. Minutos/horas desde la última actualización de vacunas
f. Fecha y horario de la última verificación ejecutada en la máquina;
g. Versión del antimalware instalado en la máquina;
h. Si es necesario reiniciar la computadora para aplicar cambios;
i. Fecha y horario de cuando la máquina fue encendida;
j. Cantidad de virus encontrados (contador) en la máquina;
k. Nombre de la computadora;
l. Dominio o grupo de trabajo de la computadora;
m. Fecha y horario de la última actualización de vacunas;
n. Sistema operativo con Service Pack;
o. Cantidad de procesadores;
p. Cantidad de memoria RAM;
q. Usuario(s) conectados en ese momento, con información de contacto (si están disponibles en el Active Directory)
r. Dirección IP;
s. Aplicativos instalados, inclusive aplicativos de terceros, con historial de instalación, conteniendo fecha y hora que el software fue instalado o removido.

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

5.2.2.18. Capacidad de reconectar equipos informáticos clientes al servidor administrativo más próximo, basado en reglas de conexión como:
a. Cambio de gateway;
b. Cambio de subnet DNS;
c. Cambio de dominio;
d. Cambio de servidor DHCP;
e. Cambio de servidor DNS;
f. Cambio de servidor WINS;
g. Aparición de nueva subnet;

5.2.2.19. Capacidad de instalar otros servidores administrativos para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes;

5.2.2.20. Capacidad de interrelacionar servidores en estructura de jerarquía para obtener informes sobre toda la estructura de endpoints;

5.2.2.21. Capacidad de herencia de tareas y políticas en la estructura jerárquica de servidores administrativos;

5.2.2.22. Capacidad de elegir cualquier computadora cliente como repositorio de vacunas y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red;

5.2.2.23. Capacidad de hacer de este repositorio de vacunas un gateway para conexión con el servidor de administración, para que otras máquinas que no logran conectarse directamente al servidor puedan usar este gateway para recibir y enviar informaciones al servidor administrativo.

5.2.2.24. Capacidad de exportar informes para los siguientes tipos de archivos: PDF, HTML y XML.

5.2.2.25. Capacidad de generar traps SNMP para monitoreo de eventos;

5.2.2.26. Capacidad de enviar correos electrónicos para cuentas específicas en caso de algún evento;

5.2.2.27. Debe tener documentación de la estructura del banco de datos para generación de informes a partir de herramientas especificas de consulta (Crystal Reports, por ejemplo).

5.2.2.28. Capacidad de conectar máquinas vía Wake on Lan para realización de tareas (barrido, actualización, instalación, etc.), inclusive de máquinas que estén en subnets diferentes del servidor);

5.2.2.29. Capacidad de habilitar automáticamente una política en caso de que ocurra una epidemia en la red (basado en cantidad de malware encontrados en determinado intervalo de tiempo);

5.2.2.30. Capacidad de realizar actualización incremental de vacunas en las computadoras clientes;

5.2.2.31. Capacidad de diferenciar máquinas virtuales de máquinas físicas;
5.2.2.32. La solución debe poder enviar notificaciones por correo electrónico.
5.2.2.33. La solución debe tener diferentes funciones de administrador que tengan una única interfaz / tablero durante el inicio de sesión y controladas por privilegios y derechos en función de sus roles (Administrador, Revisor, Investigador, etc.).
5.2.2.34. Capacidad de, en caso de epidemia, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.

5.2.3. Las funcionalidades específicas de la solución de seguridad informática tipo antivirus para la protección de computadoras tipo desktop y laptops serán los siguientes:

5.2.3.1. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota;
5.2.3.2. Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo).
5.2.3.3. Capacidad de automáticamente deshabilitar el Firewall de Windows (en caso de que exista) durante la instalación, para evitar incompatibilidad con el Firewall de la solución;
5.2.3.4. Capacidad de detección de presencia de antimalware de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación;
5.2.3.5. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antimalware, (ej.: "Win32.Trojan.banker") para que cualquier objeto detectado con el resultado elegido sea ignorado;
5.2.3.6. Capacidad de agregar aplicativos a una lista de "aplicativos confiables", donde las actividades de red, actividades de disco y acceso al registro de Windows no serán monitoreadas;
5.2.3.7. Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks);
5.2.3.8. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;
5.2.3.9. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antimalware debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;
5.2.3.10. Capacidad de verificar solamente archivos nuevos y modificados;
5.2.3.11. Capacidad de verificar objetos usando heurística;
5.2.3.12. Capacidad de agendar una pausa en la verificación;
5.2.3.13. Antes de cualquier intento de desinfección o exclusión permanente, el antimalware debe realizar un respaldo del objeto.
5.2.3.14. Capacidad de verificar correos electrónicos recibidos y enviados en los protocolos POP3, IMAP, NNTP, SMTP y MAPI, así como conexiones cifradas (SSL) para POP3 y IMAP (SSL);
5.2.3.15. Capacidad de verificar enlaces introducidos en correos electrónicos contra phishings;
5.2.3.16. Capacidad de verificación del cuerpo del correo electrónico y adjuntos usando heurística;
5.2.3.17. En caso de que el correo electrónico contenga código que parece ser, pero no es definitivamente malicioso, este debe mantenerse en cuarentena.
5.2.3.18. Posibilidad de verificar solamente correos electrónicos recibidos, o recibidos y enviados.
5.2.3.19. Capacidad de filtrar adjuntos de correos electrónicos, borrándolos o renombrándolos de acuerdo con la configuración hecha por el administrador.

5.2.3.20. Capacidad de verificación de tráfico HTTP y cualquier script de Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;
5.2.3.21. Capacidad de modificar las puertas monitoreadas por los módulos de web y correo electrónico;
5.2.3.22. En la verificación de tráfico web, en caso de que se encuentre código malicioso el programa debe:
a. Preguntar qué hacer, o;
b. Bloquear el acceso al objeto y mostrar un mensaje sobre el bloqueo, o;
c. Permitir acceso al objeto;
5.2.3.23. El antimalware de web debe realizar la verificación de, como mínimo, dos maneras diferentes, a elección del administrador:
a. Verificación on-the-fly, donde los datos se verifican mientras son recibidos en tiempo real, o;
b. Verificación de buffer, donde los datos se reciben y son almacenados para posterior verificación.
5.2.3.24. Posibilidad de agregar sitios de la web en una lista de exclusión, donde no serán verificados por el antimalware de web.
5.2.3.25. Debe tener módulo que analice las acciones de cada aplicación en ejecución en la computadora, grabando las acciones ejecutadas y comparándolas con secuencias características de actividades peligrosas. Tales registros de secuencias deben ser actualizados conjuntamente con las vacunas.
5.2.3.26. Debe tener módulo que analice cada macro de VBA ejecutado, buscando señales de actividad maliciosa.
5.2.3.27. Debe contar con módulo que analice cualquier intento de edición, exclusión o grabación del registro, de forma que sea posible elegir claves específicas para ser monitoreadas y/o bloqueadas.
5.2.3.28. Debe tener módulo de bloqueo de Phishing, con actualizaciones incluidas en las vacunas, obtenidas por Anti-Phishing Working Group (http://www.antiphishing.org/).
5.2.3.29. Capacidad de distinguir diferentes subnets y brindar opción de activar o no el firewall para una subnet específica;
5.2.3.30. Debe tener módulo IDS (Intrusion Detection System) para protección contra port scans y exploración de vulnerabilidades de software. La base de datos de análisis debe actualizarse conjuntamente con las vacunas.
5.2.3.31. El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:
a. Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas;
b. Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados.
5.2.3.32. Debe tener módulo que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínimo:
a. Discos de almacenamiento locales
b. Almacenamiento extraíble
c. Impresoras
d. CD/DVD
e. Drives de disquete
f. Modems
g. Dispositivos de cinta
h. Dispositivos multifuncionales
i. Lectores de smart card
j. Dispositivos de sincronización vía ActiveSync (Windows CE, Windows Mobile, etc.)
k. Wi-Fi
l. Adaptadores de red externos
m. Dispositivos MP3 o smartphones

n. Dispositivos Bluetooth

5.2.3.33. Capacidad de liberar acceso a un dispositivo específico y usuarios específicos por un período de tiempo específico, sin la necesidad de deshabilitar la protección, sin deshabilitar el gerenciamiento central o de intervención local del administrador en la máquina del usuario.

5.2.3.34. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por usuario.

5.2.3.35. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por agendamiento.

5.2.3.36. Capacidad de configurar nuevos dispositivos por Class ID/Hardware ID

5.2.3.37. Capacidad de limitar el acceso a sitios de internet por categoría, por contenido (video, audio, etc.), con posibilidad de configuración por usuario o grupos de usuarios y agendamiento.

5.2.3.38. Capacidad de limitar la ejecución de aplicativos por hash MD5, nombre del archivo, versión del archivo, nombre del aplicativo, versión del aplicativo, fabricante/desarrollador, categoría (ej.: navegadores, gerenciador de download, juegos, aplicación de acceso remoto, etc.).

5.2.3.39. Capacidad de bloquear la ejecución de un aplicativo que esté en almacenamiento externo.

5.2.3.40. Capacidad de limitar el acceso de los aplicativos a recursos del sistema, como claves de registro y carpetas/archivos del sistema, por categoría, fabricante o nivel de confianza del aplicativo.

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

5.2.3.42. Capacidad de, en caso de que la computadora cliente salga de la red corporativa, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.

5.2.3.43. Para los equipos informáticos con sistema operativo Windows se debe proporcionar las siguientes medidas de seguridad:

a. Antimalware de archivos residente (antispyware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
b. Antimalware de web (módulo para verificación de sitios y downloads contra virus)
c. Antimalware de correo electrónico (módulo para verificación de correos recibidos y enviados, así como sus adjuntos)
d. Firewall con IDS
e. Autoprotección (contra ataques a los servicios/procesos del antimalware)
f. Control de dispositivos externos
g. Control de acceso a sitios por categoría
h. Control de ejecución de aplicativos
i. Control de vulnerabilidades de Windows y de los aplicativos instalados.
j. La solución deberá tener la capacidad de realizar un borrado remoto de datos.

5.2.4. Las funcionalidades específicas de la solución de seguridad informática tipo antivirus para la protección de servidores con sistema operativo Windows serán los siguientes:

5.2.4.1. Compatibilidad con Sistemas Operativos Windows Server 2008 R2, 2012, 2016 y superior (64 bits).

5.2.4.2. Debe proporcionar las siguientes protecciones:

a. Antimalware de archivos residente (antispyware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
b. Autoprotección contra ataques a los servicios/procesos del antimalware

c. Firewall con IDS

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

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

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

a. Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);
b. Gerenciamiento de tarea (crear o excluir tareas de verificación)
c. Lectura de configuraciones
d. Modificación de configuraciones
e. Gerenciamiento de respaldo y cuarentena
f. Visualización de informes
g. Gerenciamiento de informes
h. Gerenciamiento de claves de licencia
i. Gerenciamiento de permisos (agregar/excluir permisos superiores)

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

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

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

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

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

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

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

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

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

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

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

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

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

5.2.4.18. Capacidad de verificar solamente archivos nuevos y modificados;

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

5.2.4.20. Capacidad de verificar objetos usando heurística;
5.2.4.21. Capacidad de configurar diferentes acciones para diferentes tipos de amenazas;
5.2.4.22. Capacidad de agendar una pausa en la verificación;
5.2.4.23. Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo;
5.2.4.24. Antes de cualquier intento de desinfección o exclusión permanente, el antimalware debe realizar un respaldo del objeto.
5.2.4.25. Debe contar con módulo que analice cada script ejecutado, buscando señales de actividad maliciosa.

5.2.5. Las funcionalidades específicas de la solución de seguridad informática tipo antivirus para la protección de servidores con sistema operativo con kernel Linux serán los siguientes:

5.2.5.1. Compatibilidad con Sistemas Operativos GNU/Linux (Red Hat/CentOS, Ubuntu/Debian) (32 y 64 bits)
5.2.5.2. Debe proporcionar las siguientes protecciones:
a. Antimalware de archivos residente (antispyware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
b. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.
5.2.5.3. Capacidad de configurar el permiso de acceso a las funciones del antimalware con, como mínimo, opciones para las siguientes funciones:
5.2.5.4. Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);
5.2.5.5. Gerenciamiento de respaldo: Creación de copias de los objetos infectados en un reservorio de respaldo antes del intento de desinfectar o eliminar tal objeto, siendo de esta manera posible la recuperación de objetos que contengan informaciones importantes;
5.2.5.6. Gerenciamiento de cuarentena: Cuarentena de objetos sospechosos y corrompidos, guardando tales archivos en una carpeta de cuarentena;
5.2.5.7. Verificación por agendamiento: búsqueda de archivos infectados y sospechosos (incluyendo archivos dentro de un rango especificado); análisis de archivos; desinfección o eliminación de objetos infectados.
5.2.5.8. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otros softwares;
5.2.5.9. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;
5.2.5.10. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antimalware debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;
5.2.5.11. Capacidad de verificar objetos usando heurística;
5.2.5.12. Control de dispositivos conectados con limitaciones de tiempo y de usuario a través de Samba Active Directory y Microsoft Active Directory en la tarea Control de dispositivos.
5.2.5.13. Administración del acceso de los usuarios a los dispositivos instalados o conectados por tipo de dispositivo y buses de conexión.
5.2.5.14. Escaneo del tráfico HTTP / HTTPS y FTP entrante del equipo del usuario y la detección de direcciones web maliciosas y suplantación de identidad (phishing).

5.2.6. El proveedor proveerá los materiales tipo cableado, conectores u otros necesarios para el cumplimiento de las actividades tipificadas en el numeral 5.1, en coordinación con la DIRTEL.

5.3. Recursos y facilidades a ser provistos por la Entidad

5.3.1. La Jefatura del Departamento de Administración de Redes y Ciberseguridad brindará las facilidades y accesos para el cumplimiento del servicio requerido.
5.3.2. La Entidad brindará una máquina virtual para la instalación de la solución de doble factor del VPN en coordinación con la DIRTEL. Dicha máquina virtual deberá poseer las siguientes características: 2 vCPU , 4GB de RAM y 200GB de disco.

5.4. Reglamentos sanitarios nacionales

El personal de la empresa adjudicada, que tengan contacto y/o realice actividades de distinta índole (tramite documentario, entrega de material, abastecimiento, brindar servicios o prestaciones, entre otros), dentro de las instalaciones de la Marina de Guerra del Perú, emitirán Declaración Jurada de toma de conocimiento y cumplimiento a los protocolos sanitarios siguientes:

5.4.1. Aislamiento COVID-19.- Procedimiento a responsabilidad de las empresas adjudicadas u otras actividades de distinta índole, por el cual una persona con caso sospechoso, reactivo en la prueba rápida o positivo en la Prueba PCR para COVID-19 será aislado y evacuado en forma inmediata al Centro de Salud para su evaluación correspondiente, debiendo elevar el respectivo informe médico por el postor adjudicado, donde se detallará las indicaciones dadas por la parte médica y su alta médica respectiva.
5.4.2. Distanciamiento Social.- Aumentar el espacio que separa a las personas y reducir la frecuencia de contacto, con el fin de reducir la transmisión de la enfermedad (distancia mínima de DOS (2) metros aproximadamente.
5.4.3. Higiene Respiratoria. - Cubrirse la boca y nariz con UNA (1) tapa boca certificado y aprobado por el MINSA, en todo momento y de manera obligatoria.
5.4.4. Higiene de manos.- Uso de guantes y lavado de manos a menudo con agua y jabón o solución recomendada; de acuerdo a la naturaleza de su visita, de manera obligatoria.
5.4.5. Higiene Ambiental. Mantener la limpieza de los lugares, superficies y movilidades de trabajo, de manera constante y obligatoria.

Asimismo, los postores deberán presentar declaración jurada donde se detalle que el personal a su cargo no presenta sintomatología o haber estado en contacto de personas infectadas con COVID-19, con el propósito de descartar cualquier contagio del personal de la Marina de Guerra del Perú, el postor dará cumplimiento a dispuesto en la Resolución N° 283-2020 MINSA de fecha 13 de mayo del 2020, en lo referente a trabajadores con riesgo y alto riesgo a exposición COVID-19, donde se detalla al personal vulnerable las características de este tipo de personas, las cuales son:

- Mayores de 65 años
- Embarazadas y lactantes
- Enfermos cardiovasculares
- Pacientes con cáncer y/o diabetes mellitus
- Obesos con IMC de 40 a mas
- Asmáticos moderados o graves
- Enfermos respiratorios crónicos
- Enfermos pulmonares crónicos
- Insuficientes renales crónicos en tratamientos con hemodiálisis
- Enfermos o en tratamiento con inmunosupresores
- Otros, bajo responsabilidad del postor adjudicado.

Se aplicará lo establecido según Resolución Ministerial Nro. 265-2020 MINSA de fecha 7 de mayo del 2020, modificada por Resolución Ministerial Nro. 283-2020 MINSA de fecha 13 de mayo del 2020.

5.5. Prestaciones accesorias a la prestación principal

5.5.1. Mantenimiento preventivo

5.5.1.1. Se efectuará el mantenimiento preventivo (helpchecking) de la solución de seguridad informática tipo antivirus en forma semestral y en coordinación con la Dirección de Telemática de la Marina.

5.5.2. Soporte técnico

5.5.2.1. Se efectuará el soporte técnico vía telefónica, correo electrónico o sesión remota, tipo 24x7x365, es decir durante las 24 horas del día, los 7 días de la semana y los 365 días del año, con un tiempo máximo de respuesta de 4 horas. En caso no se pudiera solucionar un incidente a través de los medios antes descritos luego de 48 horas de transcurrido el incidente, el soporte técnico deberá realizarse en forma presencial.
5.5.2.2. Deberá asegurarse el acceso permanente y oportuno a las actualizaciones de seguridad y de rendimiento de la solución de seguridad informática tipo antivirus ofertado, parcial o integral, proporcionado por el fabricante.
5.5.2.3. Se efectuará evaluaciones de mejora y/o prevención para la solución de seguridad informática tipo antivirus, parcial o integral.
5.5.2.4. Se efectuará la ejecución de un ASSESSMENT DE SEGURIDAD con una herramienta de pentesting a la solución de seguridad informática tipo antivirus por única vez y en forma coordinada con la Dirección de Telemática de la Marina.
5.5.2.5. Efectuará el escalamiento de soporte a nivel fabricante cuando lo requiera la Dirección de Telemática de la Marina.
5.5.2.6. Deberá proporcionar alternativas de solución para no afectar la continuidad del servicio por un plazo no mayor a 72 horas.

5.5.3. Capacitación

5.5.3.1. Se efectuará la capacitación en administración y despliegue de la solución de seguridad informática tipo antivirus, el cual estará dirigido a un mínimo de TRES (3) técnicos de la División de Ciberseguridad de la DIRTEL, con un tiempo mínimo de duración de 8 horas, a realizarse en las instalaciones de la Entidad, o en forma virtual, dentro de los 3 meses posteriores a la culminación de las actividades tipificadas en el numeral 5.1.
5.5.3.2. El sylabus corresponderá a la versión de la solución de seguridad informática tipo antivirus implementada y será elaborado por el proveedor en coordinación con la DIRTEL.
5.5.3.3. El material a entregar deberá contemplar el detalle de todos los temas a dictarse según el sylabus.
5.5.3.4. Se deberá otorgar constancias de participación para el personal que siga la capacitación.

5.5.4. Garantía

5.5.4.1. El proveedor presentará la garantía de buen funcionamiento será por el mismo periodo de vigencia del licenciamiento. Asimismo, iniciará al mismo tiempo que la vigencia del licenciamiento del software de seguridad implementado por el proveedor.
5.5.4.2. La garantía de buen funcionamiento comprende que la solución ofertada cumpla con todos los requerimientos tipificados en el presente documento.

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

5.6. Lugar y plazo de la prestación

5.6.1. Lugar

La prestación del servicio será en la Dirección de Telemática de la Marina, cito en Av. La Marina Cdra. 36 S/N, dentro de la Estación Naval La Perla.

5.6.2. Plazo

5.6.2.1. El plazo para la configuración del servicio del periodo comprendido entre el años 2021 - 2022, será de 20 días calendario, contabilizados a partir del día siguiente de la firma del contrato.
5.6.2.2. La configuración del servicio del periodo comprendido entre el años 2022 – 2023 y 2023 - 2024, será de máximo 10 días calendarios antes de la caducidad de la licencia vigente.
5.6.2.3. El plazo de ejecución del servicio es de 1,095 días calendarios, dividido en tres periodos de 365 días calendarios entre los años 2021 y 2024, los mismos que corresponden a la duración del licenciamiento anual a ser expedidas.

5.7. Confidencialidad

El POSTOR deberá firmar el Acta de Confidencialidad proporcionado por la Dirección de Telemática de la Marina, para el desarrollo de los trabajos de soporte técnico y otros que se realicen sobre los sistemas informáticos de la Institución, el cual se realizará a la firma del contrato.

El acuerdo de confidencialidad formará parte del contrato a fin de permitir y resguardar la Información clasificada de la Institución, pudiéndose limitar el acceso de profesionales que puedan afectar a la seguridad de la Institución.

5.8. Medidas de control durante la ejecución contractual

5.8.1. Designación de responsabilidades

5.8.1.1. Áreas que coordinarán con el proveedor: La Jefatura del Departamento de Administración de Redes y Ciberseguridad y la División de Ciberseguridad.
5.8.1.2. Área responsable de las medidas de control: La Jefatura del Departamento de Administración de Redes y Ciberseguridad.
5.8.1.3. Área que brindará la conformidad: La Jefatura de la División de Ciberseguridad.

5.8.2. Medidas de control

5.8.2.1. Supervisará que el proveedor cumpla con todo lo requerido en el presente documento.
5.8.2.2. Verificará la correcta confección del Acta de Conformidad.

5.8.3. Conformidad

Se elaborarán Actas de Conformidad en forma anual, posterior a la configuración del servicio de licenciamiento requerido, debiendo contener los siguientes documentos:

5.8.3.1. Screenshot del portal oficial del fabricante donde figuren las claves u otros indicadores que permita validar la licencia proporcionada.
5.8.3.2. Informe elaborado por el proveedor donde acredite el cumplimiento de lo tipificado en el numeral 5.1.
5.8.3.3. Declaración jurada del proveedor en el cual se compromete a brindar el mantenimiento preventivo, soporte técnico, capacitación y garantía de buen funcionamiento, de acuerdo a lo tipificado del numeral 5.5.1 al numeral 5.5.4. En dicho documento el proveedor deberá indicar los teléfonos y correos electrónicos para contacto.

5.9. Forma de pago

El pago se realizará en TRES (03) armadas, previa presentación del acta de conformidad detallada en el numeral 5.9.3, de acuerdo a lo siguiente:

5.9.1. El primer pago se efectuará en el año 2021 y corresponderá al 33.33% del monto contractual.
5.9.2. El segundo pago se efectuará en el año 2022 y corresponderá al 33.33% del monto contractual.
5.9.3. El segundo pago se efectuará en el año 2023 y corresponderá al 33.34% del monto contractual.

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

ÍTEM N°5
SERVICIO DE LICENCIAMIENTO PARA EL SISTEMA DE SEGURIDAD INFORMÁTICA FIREWALL DE BASE DE DATOS

I. TÉRMINOS DE REFERENCIA

1. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de licenciamiento para el Sistema de Seguridad Informática Firewall de Base de Datos.

2. FINALIDAD PÚBLICA

El presente proceso busca continuar brindando seguridad a su información, a través del uso de un equipo appliance especializado para la detección y remediación ante ataques a las bases de datos con los que cuenta la Institución, para el almacenamiento de información crítica y sensible.

3. ANTECEDENTES

La Entidad, dentro de su estrategia de seguridad de la información institucional, posee un conjunto de soluciones de seguridad informática que permiten proteger la información que se encuentra almacenada en los diferentes equipos informáticos, estaciones de trabajo y servidores.

En tal sentido, el presente proceso se enfoca en renovar y continuar brindando seguridad informática a través de la detección de ataques dirigidos a los servidores de aplicaciones de la Institución. Para ello, se cuenta con un equipo appliance denominado firewall de base de datos, el cual protege con características especiales, las bases de datos que son componentes esenciales de los sistemas de información críticos para la Institución.

4. OBJETIVO DE LA CONTRATACIÓN

Mantener el nivel de seguridad de la información de la Entidad a través de la renovación del licenciamiento del equipo appliance firewall de base de datos.

5. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

5.1. Actividades

Las siguientes actividades serán realizadas en forma anual, en cumplimiento a la contratación del servicio y en coordinación con la Dirección de Telemática de la Marina, en adelante DIRTEL:

5.1.1. Generación de las licencias correspondientes al appliance firewall de base de datos y la remisión a la DIRTEL.
5.1.2. Instalación y/o configuración de la solución propuesta de ser requerido.
5.1.3. Instalación de la nueva licencia en la solución.
5.1.4. Revisión y/u optimización integral de la solución.

5.2. Recursos a ser provistos por el proveedor

5.2.1. TRES (3) licenciamientos anuales (vigencia de 365 días cada uno) del equipo appliance firewall de base de datos a nombre de la Marina de Guerra del Perú.
5.2.2. Las características generales relacionadas a las capacidades que brinda el licenciamiento serán las siguientes:

5.2.2.1. Deberá tener licenciamiento para al menos 25 Servidores con motor MSSQL Server.
5.2.2.2. Soportar al menos el almacenamiento de información de 1TB de Información.
5.2.2.3. El software utilizado no debe generar una carga adicional superior al 5% de la actividad del CPU del servidor con la base de datos analizada.
5.2.2.4. No se debe generar una afectación mayor a un 5% en el tiempo de respuesta de la base de datos analizada.
5.2.2.5. Filtrar las peticiones que llegan al manejador de bases de datos mediante un conjunto de reglas preestablecidas y editables.
5.2.2.6. Alerta y bloquea ataques de base de datos y solicitudes de acceso anormales, en tiempo real incluyendo Inyecciones de SQL, desbordamiento de búfer, denegación de servicios y más.
5.2.2.7. Permitir el licenciamiento futuro para el soporte de plataformas compatibles de bases de datos ORACLE SQL, MYSQL entre otros.
5.2.2.8. Capacidad de proteger bases de datos tanto en servidores físicos como en servidores virtuales o ambos de manera paralela.

5.2.3. Las características relacionadas a la protección de base de datos serán las siguientes:

5.2.3.1. Capacidad de ubicar información confidencial en base de datos y validar la línea base de esos sistemas en términos de configuración, usuarios, permisos, objetos, etc.
5.2.3.2. Para la configuración de la base de datos, usuarios, roles, privilegios y objetos de la misma, proveer:
a. Informe del estado actual de la configuración base.
b. Capacidad de automatizar la toma de instantáneas en forma programada con el objeto de identificar y reportar cualquier cambio en la configuración base.
c. Capacidad de comparar dos instancias de bases de datos y reportar cualquier diferencia en la configuración base.
5.2.3.3. Permitir establecer un control estricto sobre los cambios. Debe incluir procesos para aprobar los cambios, así como controles de seguimiento para identificar cambios y validar que hayan sido aprobados.
5.2.3.4. Debe permitir controlar la actividad bajo control de cambios, la actividad del administrador, las sesiones de usuario y la actividad sobre los datos.
5.2.3.5. La herramienta debe tener la capacidad de definir reglas para bloquear la actividad de sentencias especificas de SQL, incluyendo:
a. Usuarios privilegiados accediendo información correspondiente a los aplicativos.
b. Conexiones diferentes a las realizadas por las aplicaciones autorizadas (definidas con base al programa y máquina remota).
c. Acceso a información privilegiada por aplicaciones diferentes a las autorizadas (definidas con base al programa y máquina remota).
d. Delimitación de responsabilidades: evitar que usuarios privilegiados puedan crear usuarios, modificar atributos de usuarios, brindar roles o privilegios, etc., excepto cuando exista una aprobación temporal por parte de los administradores de seguridad dentro de la organización.
5.2.3.6. Permitir generar reportes de cumplimiento de diversas normativas.
5.2.3.7. Debe permitir auditoria forense para visualizar lo que ocurre dentro de las bases de datos.
5.2.3.8. Deberá detectar anomalías con el fin de comparar la actividad actual vs actividad realizada en el pasado para poder identificar posibles ataques.
5.2.3.9. Capacidad de detección de anomalías que permita detectar inyecciones de SQL, cuentas comprometidas.
5.2.3.10. Detección de usuarios privilegiados con el objetivo evitar que los administradores accedan y ganen visibilidad sobre los datos, al mismo

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

tiempo que provee la capacidad de separar funciones que mitiguen riesgos de actividades de usuarios privilegiados.
5.2.3.11. Permitir generar listas blancas y negras según la fuente de la actividad
5.2.3.12. Permite limitar la tasa de extracción de datos basado, día y hora y filtros basados en el contenido de la actividad.

5.2.4. Las características relacionadas al monitoreado y captura de actividades serán las siguientes:

5.2.4.1. Se debe proveer un mecanismo para capturar toda la actividad dentro de la base de datos analizada, incluyendo:
5.2.4.2. Conexiones encriptadas.
a. Conexiones remotas.
b. Conexiones locales.
c. Conexiones vía TCP, memoria compartida o "named pipes" para el caso de Microsoft SQL.
d. Actividad interna en la base de datos incluyendo PL/SQL (Oracle), TSQL (Microsoft SQL), triggers, etc. incluso con la sentencia "execute immediate" o "sp_executesiq".
e. Todos los queries, DDLs y DMLs
f. Toda la actividad de las cuentas administrativas, incluyendo SYS y SA.
g. Toda la actividad generada por aplicaciones, tareas y sentencias SQL (incluyendo APEX para bases de datos Oracle)
h. Cualquier actividad dentro de la base de datos.
i. En el caso particular de Microsoft SQL se debe poder capturar:
i) Ejecución de tareas vía el "Oracle job scheduler" o el agente de SQL.
ii) Actividad de Java VM o .NET VM que se ejecute dentro de la base de datos monitoreada.
5.2.4.3. Descubrimiento, monitoreo y captura de actividad de cualquier tipo de usuarios, ejecución de sentencias y ataques.
5.2.4.4. Capacidad de enviar reportes y alertas por correo electrónico.
5.2.4.5. Deben ser generados al menos en los formatos HTML y PDF.
5.2.4.6. El producto debe poder enviar sus reportes de actividad a cualquier sistema SIEM.

5.2.5. Las características relacionadas al provisionamiento de información entre bases de datos serán las siguientes:

5.2.5.1. Debe tener la capacidad de realizar una copia de una base de datos productiva hacia una base de datos no-productiva.
5.2.5.2. La base de datos copiada debe ser utilizable y por lo tanto debe incluir:
a. Copia de todas las tablas, índices, procedimientos, triggers, y cualquier otro objeto de la base de datos.
b. El manejo de llaves foráneas entre las tablas.
c. El manejo de cualquier otra dependencia entre objetos.
5.2.5.3. En forma adicional a la copia completa, la herramienta debe poder extraer solamente una porción de la base de datos productiva hacia una base de datos no-productiva (por ejemplo, copiar solamente el 20%).
5.2.5.4. Cuando se copie una porción de la base de datos productiva, como una tabla que contenga llaves foráneas, solamente deben ser copiada la información relevante a las tablas en cuestión.
5.2.5.5. La copia de información debe ser realizada directamente entre las bases de datos origen y destino, sin almacenar información en alguna otra ubicación temporal o definitiva, y sin utilizar respaldos o información previamente exportada.

5.2.6. Con la finalidad que el proveedor cumpla con proporcionar una solución de firewall de base de datos de acuerdo a las exigencias técnicas requeridas en el presente documento durante el plazo establecido, se aceptará la reposición y/o inclusión de

hardware tipo appliance necesario. Para tal efecto, se deberá tener en cuenta las diferentes vigencias tecnológicas publicadas por el fabricante en sus canales de comunicación oficiales.

5.2.7. El proveedor proveerá los materiales tipo cableado, conectores u otros necesarios para el cumplimiento de las actividades tipificadas en el numeral 5.1, en coordinación con la DIRTEL.

5.3. Recursos y facilidades a ser provistos por la Entidad

5.3.1. La Jefatura del Departamento de Administración de Redes y Ciberseguridad brindará las facilidades y accesos para el cumplimiento del servicio requerido.

5.4. Reglamentos sanitarios nacionales

El personal de la empresa adjudicada, que tengan contacto y/o realice actividades de distinta índole (tramite documentario, entrega de material, abastecimiento, brindar servicios o prestaciones, entre otros), dentro de las instalaciones de la Marina de Guerra del Perú, emitirán Declaración Jurada de toma de conocimiento y cumplimiento a los protocolos sanitarios siguientes:

5.4.1. Aislamiento COVID-19.- Procedimiento a responsabilidad de las empresas adjudicadas u otras actividades de distinta índole, por el cual una persona con caso sospechoso, reactivo en la prueba rápida o positivo en la Prueba PCR para COVID-19 será aislado y evacuado en forma inmediata al Centro de Salud para su evaluación correspondiente, debiendo elevar el respectivo informe médico por el postor adjudicado, donde se detallará las indicaciones dadas por la parte médica y su alta médica respectiva.

5.4.2. Distanciamiento Social.- Aumentar el espacio que separa a las personas y reducir la frecuencia de contacto, con el fin de reducir la transmisión de la enfermedad (distancia mínima de DOS (2) metros aproximadamente.

5.4.3. Higiene Respiratoria. - Cubrirse la boca y nariz con UNA (1) tapa boca certificado y aprobado por el MINSA, en todo momento y de manera obligatoria.

5.4.4. Higiene de manos.- Uso de guantes y lavado de manos a menudo con agua y jabón o solución recomendada; de acuerdo a la naturaleza de su visita, de manera obligatoria.

5.4.5. Higiene Ambiental. Mantener la limpieza de los lugares, superficies y movilidades de trabajo, de manera constante y obligatoria.

Asimismo, los postores deberán presentar declaración jurada donde se detalle que el personal a su cargo no presenta sintomatología o haber estado en contacto de personas infectadas con COVID-19, con el propósito de descartar cualquier contagio del personal de la Marina de Guerra del Perú, el postor dará cumplimiento a dispuesto en la Resolución Nº 283-2020 MINSA de fecha 13 de mayo del 2020, en lo referente a trabajadores con riesgo y alto riesgo a exposición COVID-19, donde se detalla al personal vulnerable las características de este tipo de personas, las cuales son:

- Mayores de 65 años
- Embarazadas y lactantes
- Enfermos cardiovasculares
- Pacientes con cáncer y/o diabetes mellitus
- Obesos con IMC de 40 a mas
- Asmáticos moderados o graves
- Enfermos respiratorios crónicos
- Enfermos pulmonares crónicos

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

- Insuficientes renales crónicos en tratamientos con hemodiálisis
- Enfermos o en tratamiento con inmunosupresores
- Otros, bajo responsabilidad del postor adjudicado.

Se aplicará lo establecido según Resolución Ministerial Nro. 265-2020 MINSA de fecha 7 de mayo del 2020, modificada por Resolución Ministerial Nro. 283-2020 MINSA de fecha 13 de mayo del 2020.

5.5. Prestaciones accesorias a la prestación principal

5.5.1. Mantenimiento preventivo

5.5.1.1. Se podrá requerir el mantenimiento preventivo al appliance en forma semestral y en coordinación con la Dirección de Telemática de la Marina.

5.5.2. Soporte técnico

5.5.2.1. Se podrá requerir soporte técnico vía telefónica, correo electrónico o sesión remota, tipo 24x7x365, es decir durante las 24 horas del día, los 7 días de la semana y los 365 días del año, con un tiempo máximo de respuesta de 4 horas. En caso no se pudiera solucionar un incidente a través de los medios antes descritos luego de 48 horas de transcurrido el incidente, el soporte técnico deberá realizarse en forma presencial.

5.5.2.2. Deberá asegurarse el acceso permanente y oportuno a las actualizaciones de seguridad y de rendimiento del equipo appliance firewall de base de datos ofertado, parcial o integral, proporcionado por el fabricante.

5.5.2.3. Se podrá requerir evaluaciones de mejora y/o prevención para el equipo appliance firewall de base de datos, parcial o integral.

5.5.2.4. Se podrá requerir la ejecución de un ASSESSMENT DE SEGURIDAD con una herramienta de pentesting al equipo appliance firewall de base de datos por única vez y en forma coordinada con la Dirección de Telemática de la Marina.

5.5.2.5. Efectuará el escalamiento de soporte a nivel fabricante cuando lo requiera la Dirección de Telemática de la Marina.

5.5.2.6. Deberá proporcionar alternativas de solución para no afectar la continuidad del servicio por un plazo no mayor a 72 horas.

5.5.3. Capacitación

5.5.3.1. Se podrá requerir la capacitación en administración del equipo appliance firewall de base de datos, el cual estará dirigido a un mínimo de TRES (3) técnicos de la División de Ciberseguridad de la DIRTEL, con un tiempo mínimo de duración de 8 horas, a realizarse en las instalaciones de la Entidad, o en forma virtual, dentro de los 3 meses posteriores a la culminación de las actividades tipificadas en el numeral 5.1.

5.5.3.2. El sylabus corresponderá a la versión del equipo appliance firewall de base de datos implementada y será elaborado por el proveedor en coordinación con la DIRTEL.

5.5.3.3. El material a entregar deberá contemplar el detalle de todos los temas a dictarse según el syllabus.

5.5.3.4. Se deberá otorgar constancias de participación para el personal que siga la capacitación.

5.5.4. Garantía

5.5.4.1. El proveedor presentará la garantía de buen funcionamiento será por el mismo periodo de vigencia del licenciamiento. Asimismo, iniciará al mismo

tiempo que la vigencia del licenciamiento del software de seguridad implementado por el proveedor.

5.5.4.2. La garantía de buen funcionamiento comprende que la solución ofertada cumpla con todos los requerimientos tipificados en el presente documento.

5.6. Lugar y plazo de la prestación

5.6.1. Lugar

La prestación del servicio será en la Dirección de Telemática de la Marina, cito en Av. La Marina Cdra. 36 S/N, dentro de la Estación Naval La Perla.

5.6.2. Plazo

5.6.2.1. El plazo para la configuración del servicio del periodo comprendido entre los años 2021 - 2022, será de 50 días calendario, contabilizados a partir del día siguiente de la firma del contrato.

5.6.2.2. La configuración del servicio del periodo comprendido entre los años 2022 – 2023 y 2023 - 2024, será de máximo 10 días calendarios antes de la caducidad de la licencia vigente.

5.6.2.3. El plazo de ejecución del servicio es de 1,095 días calendarios, dividido en tres periodos de 365 días calendarios entre los años 2021 y 2024, los mismos que corresponden a la duración del licenciamiento anual a ser expedidas.

5.7. Confidencialidad

El POSTOR deberá firmar el Acta de Confidencialidad proporcionado por la Dirección de Telemática de la Marina, para el desarrollo de los trabajos de soporte técnico y otros que se realicen sobre los sistemas informáticos de la Institución, el cual se realizará a la firma del contrato.

El acuerdo de confidencialidad formará parte del contrato a fin de permitir y resguardar la Información clasificada de la Institución, pudiéndose limitar el acceso de profesionales que puedan afectar a la seguridad de la Institución.

5.8. Medidas de control durante la ejecución contractual

5.8.1. Designación de responsabilidades

5.8.1.1. Áreas que coordinarán con el proveedor: La Jefatura del Departamento de Administración de Redes y Ciberseguridad y la División de Ciberseguridad.

5.8.1.2. Área responsable de las medidas de control: La Jefatura del Departamento de Administración de Redes y Ciberseguridad.

5.8.1.3. Área que brindará la conformidad: La Jefatura de la División de Ciberseguridad.

5.8.2. Medidas de control

5.8.2.1. Supervisará que el proveedor cumpla con todo lo requerido en el presente documento.

5.8.2.2. Verificará la correcta confección del Acta de Conformidad.

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

5.8.3. Conformidad

Se elaborarán Actas de Conformidad en forma anual, posterior a la configuración del servicio de licenciamiento requerido, debiendo contener los siguientes documentos:

5.8.3.1. Screenshot del portal oficial del fabricante donde figuren las claves u otros indicadores que permita validar la licencia proporcionada.

5.8.3.2. Informe elaborado por el proveedor donde acredite el cumplimiento de lo tipificado en el numeral 5.1.

5.8.3.3. Declaración jurada del proveedor en el cual se compromete a brindar el mantenimiento preventivo, soporte técnico, capacitación y garantía de buen funcionamiento, de acuerdo a lo tipificado del numeral 5.5.1 al numeral 5.5.4. En dicho documento el proveedor deberá indicar los teléfonos y correos electrónicos para contacto.

5.9. Forma de pago

El pago se realizará en TRES (03) armadas, previa presentación del acta de conformidad detallada en el numeral 5.9.3, de acuerdo a lo siguiente:

5.9.1. El primer pago se efectuará en el año 2021 y corresponderá al 33.33% del monto contractual.

5.9.2. El segundo pago se efectuará en el año 2022 y corresponderá al 33.33% del monto contractual.

5.9.3. El segundo pago se efectuará en el año 2023 y corresponderá al 33.34% del monto contractual.

ÍTEM N°6
SERVICIO DE RENOVACIÓN LICENCIA PARA EL ANTIMALWARE

I. TÉRMINOS DE REFERENCIA

1. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de renovación licencia para el Antimalware.

2. FINALIDAD PÚBLICA

Incrementar el nivel de seguridad de la información de la Marina de Guerra del Perú a través de la renovación del licenciamiento del sistema de seguridad informática antimalware Institucional.

3. ANTECEDENTES

La Entidad, dentro de su estrategia de seguridad de la información institucional, posee un conjunto de soluciones de seguridad informática que permiten proteger la información que se encuentra almacenada en los diferentes equipos informáticos, estaciones de trabajo y servidores.

En tal sentido, el presente proceso se enfoca en renovar y/o continuar brindando seguridad informática a través de la detección de ataques de tipo cero y/o tipo ATP, los cuales no son detectados por soluciones convencionales y resultan altamente efectivos. Para ello, se cuenta con un equipo appliance de análisis de malware tipo sandbox, el cual genera un ambiente idóneo para el análisis de tráfico sospechoso.

4. OBJETIVO DE LA CONTRATACIÓN

Mantener el nivel de seguridad de la información de la Entidad a través de la renovación del licenciamiento del equipo Antimalware.

5. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

5.1. Actividades

Las siguientes actividades serán realizadas en forma anual, en cumplimiento a la contratación del servicio y en coordinación con la Dirección de Telemática de la Marina, en adelante DIRTEL:

5.1.1. Generación de las licencias correspondientes al equipo appliance sandbox antimalware y su recepción por la DIRTEL.
5.1.2. Instalación y/o configuración de la solución propuesta, de ser requerido.
5.1.3. Instalación de nueva licencia.
5.1.4. Revisión y/u optimización integral de la solución.

5.2. Recursos a ser provistos por el proveedor

5.2.1. TRES (3) licenciamientos anuales (vigencia de 365 días cada uno) del equipo appliance sandbox antimalware, a nombre de la Marina de Guerra del Perú.

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

5.2.2. Las características relacionadas a la prevención de amenazas que permitirá el licenciamiento sobre el appliance serán las siguientes:

5.2.2.1. El licenciamiento debe permitir el funcionamiento de al menos 14 Máquinas Virtuales para sandboxing.
5.2.2.2. Deberá soportar el análisis de al menos 1 Gbps de tráfico.
5.2.2.3. Soportar al menos el análisis de 1400 ficheros por hora.
5.2.2.4. Soportar al menos el almacenamiento en disco de 1TB.
5.2.2.5. Debe poder detectar malware desconocido (ATP - Amenaza persistente avanzada y Amenazas de día cero), ransomware con filtrado avanzado de amenazas y análisis de ejecución en tiempo real, e inspección de tráfico saliente y devolución de llamada;
5.2.2.6. Debe poder recibir archivos desde otros dispositivos de seguridad y de red para su análisis en la solución instalada localmente, donde el archivo se simulará y ejecutará en un entorno controlado;
5.2.2.7. Debe admitir el análisis de archivos provenientes y enviados a Internet mediante los protocolos HTTP, FTP, SMTP, así como archivos en tránsito interno entre servidores de archivos que usan SMB. Este análisis lo puede realizar en alguno de los siguientes modos de operación: sniffer, in-line (transparente o L2) o L3;
5.2.2.8. Debe poder inspeccionar el tráfico cifrado SSL. Esta capacidad puede ser realizada mediante la integración con un firewall, IPS u otro dispositivo de red o seguridad;
5.2.2.9. Debe tener un mecanismo para identificar hosts infectados que intentan acceder a direcciones DNS de dominios maliciosos;
5.2.2.10. Debe permitir seleccionar a través de políticas qué tipos de archivos se someterán a este análisis y prevención;
5.2.2.11. Implementar e identificar la existencia de malware en archivos adjuntos de correo electrónico y URL conocidas

5.2.3. Las características relacionadas a las funcionalidades ATP que permitirá el licenciamiento sobre el appliance serán las siguientes:

5.2.3.1. Implemente la detección y el bloqueo de malware que utiliza mecanismos de escaneo en archivos PDF;
5.2.3.2. Capacidad de emular ataques en los siguientes sistemas operativos: Windows 7, Windows 8, Windows 10 y Linux de manera local, sin necesidad de enviar archivos a la nube.
5.2.3.3. Soportar el análisis de archivos Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar y class) y Linux en un entorno sandbox local sin necesidad de enviar el archivo a la nube.
5.2.3.4. Debe tener una nube de inteligencia patentada por el fabricante que sea responsable de actualizar toda la base de seguridad mediante firmas;
5.2.3.5. Debe admitir topologías de implementación en modo sniffer o en línea (in-line)
5.2.3.6. Debe admitir topologías de implementación integradas con firewalls, solución de protección de correo electrónico, waf o protección de estaciones de trabajo (endpoints);
5.2.3.7. Debe admitir topologías de implementación con adaptadores para la integración con soluciones de terceros a través del protocolo ICAP o BCC;
5.2.3.8. Debe admitir topologías de implementación que permitan el análisis de archivos compartidos, al menos mediante SMB.
5.2.3.9. Debe permitir la recepción manual de archivos a través de su consola gráfica.
5.2.3.10. Debe admitir la recepción de archivos a través de APIs.
5.2.3.11. Debe permitir la carga de máquinas virtuales personalizadas.
5.2.3.12. Todos los análisis y bloqueos de malware y/o códigos maliciosos deben realizarse en tiempo real y de manera local, sin que la muestra deba ser enviada a la nube.

5.2.3.13. Debe admitir, reglas de YARA como estándar para crear reglas para la detección de malware;
5.2.3.14. Debe tener la capacidad de crear firmas en tiempo real, para la protección contra las amenazas detectadas en base al análisis del comportamiento del malware en el entorno controlado.
5.2.3.15. Debe permitir la distribución automática de las nuevas firmas entre los dispositivos integrados: firewalls, gateway de correo electrónico, firewall de aplicaciones web, entre otros.

5.2.4. Las características relacionadas a la función de visibilidad que permitirá el licenciamiento sobre el appliance serán las siguientes:

5.2.4.1. La solución debe permitir al administrador la descarga del archivo original analizado por el Sandbox.
5.2.4.2. En caso de veredicto positivo, se debe presentar al menos la siguiente información:
a. Tipo de archivo
b. Fuente del malware (al menos la dirección IP de origen)
c. Equipo comprometido (cliente que intentó descargar el malware o acceder a la URL comprometida)
d. Descripción detallada del comportamiento del malware en el ambiente virtual.
e. Captura de pantalla o video donde se muestre el comportamiento del malware en el ambiente virtual.

5.2.5. Con la finalidad que el proveedor cumpla con proporcionar el licenciamiento necesario para las exigencias técnicas requeridas en el presente documento durante el plazo establecido, se aceptará la reposición y/o inclusión de hardware tipo appliance necesario. Para tal efecto, se deberá tener en cuenta las diferentes vigencias tecnológicas publicadas por el fabricante en sus canales de comunicación oficiales.
5.2.6. El proveedor proveerá los materiales tipo cableado, conectores u otros necesarios para el cumplimiento de las actividades tipificadas en el numeral 5.1, en coordinación con la DIRTEL.

5.3. Recursos y facilidades a ser provistos por la Entidad

La Jefatura del Departamento de Administración de Redes y Ciberseguridad brindará las facilidades y accesos para el cumplimiento del servicio requerido.

5.4. Reglamentos sanitarios nacionales

El personal de la empresa adjudicada, que tengan contacto y/o realice actividades de distinta índole (tramite documentario, entrega de material, abastecimiento, brindar servicios o prestaciones, entre otros), dentro de las instalaciones de la Marina de Guerra del Perú, emitirán Declaración Jurada de toma de conocimiento y cumplimiento a los protocolos sanitarios siguientes:

5.4.1. Aislamiento COVID-19.- Procedimiento a responsabilidad de las empresas adjudicadas u otras actividades de distinta índole, por el cual una persona con caso sospechoso, reactivo en la prueba rápida o positivo en la Prueba PCR para COVID-19 será aislado y evacuado en forma inmediata al Centro de Salud para su evaluación correspondiente, debiendo elevar el respectivo informe médico por el postor adjudicado, donde se detallará las indicaciones dadas por la parte médica y su alta médica respectiva.

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

5.4.2. Distanciamiento Social.- Aumentar el espacio que separa a las personas y reducir la frecuencia de contacto, con el fin de reducir la transmisión de la enfermedad (distancia mínima de DOS (2) metros aproximadamente.
5.4.3. Higiene Respiratoria. - Cubrirse la boca y nariz con UNA (1) tapa boca certificado y aprobado por el MINSA, en todo momento y de manera obligatoria.
5.4.4. Higiene de manos.- Uso de guantes y lavado de manos a menudo con agua y jabón o solución recomendada; de acuerdo a la naturaleza de su visita, de manera obligatoria.
5.4.5. Higiene Ambiental. Mantener la limpieza de los lugares, superficies y movilidades de trabajo, de manera constante y obligatoria.

Asimismo, los postores deberán presentar declaración jurada donde se detalle que el personal a su cargo no presenta sintomatología o haber estado en contacto de personas infectadas con COVID-19, con el propósito de descartar cualquier contagio del personal de la Marina de Guerra del Perú, el postor dará cumplimiento a dispuesto en la Resolución Nº 283-2020 MINSA de fecha 13 de mayo del 2020, en lo referente a trabajadores con riesgo y alto riesgo a exposición COVID-19, donde se detalla al personal vulnerable las características de este tipo de personas, las cuales son:

- Mayores de 65 años
- Embarazadas y lactantes
- Enfermos cardiovasculares
- Pacientes con cáncer y/o diabetes mellitus
- Obesos con IMC de 40 a mas
- Asmáticos moderados o graves
- Enfermos respiratorios crónicos
- Enfermos pulmonares crónicos
- Insuficientes renales crónicos en tratamientos con hemodiálisis
- Enfermos o en tratamiento con inmunosupresores
- Otros, bajo responsabilidad del postor adjudicado.

Se aplicará lo establecido según Resolución Ministerial Nro. 265-2020 MINSA de fecha 7 de mayo del 2020, modificada por Resolución Ministerial Nro. 283-2020 MINSA de fecha 13 de mayo del 2020.

5.5. Prestaciones accesorias a la prestación principal

5.5.1. Mantenimiento preventivo

5.5.1.1. Se podrá requerir el mantenimiento preventivo al appliance en forma semestral y en coordinación con la Dirección de Telemática de la Marina.

5.5.2. Soporte técnico

5.5.2.1. Se podrá requerir soporte técnico vía telefónica, correo electrónico o sesión remota, tipo 24x7x365, es decir durante las 24 horas del día, los 7 días de la semana y los 365 días del año, con un tiempo máximo de respuesta de 4 horas. En caso no se pudiera solucionar un incidente a través de los medios antes descritos luego de 48 horas de transcurrido el incidente, el soporte técnico deberá realizarse en forma presencial.
5.5.2.2. Deberá asegurarse el acceso permanente y oportuno a las actualizaciones de seguridad y de rendimiento del equipo appliance sandbox antimalware ofertado, parcial o integral, proporcionado por el fabricante.
5.5.2.3. Se podrá requerir evaluaciones de mejora y/o prevención para el equipo appliance sandbox antimalware, parcial o integral.
5.5.2.4. Se podrá requerir la ejecución de un ASSESSMENT DE SEGURIDAD con una herramienta de pentesting al equipo appliance sandbox antimalware por

única vez y en forma coordinada con la Dirección de Telemática de la Marina.

5.5.2.5. Efectuará el escalamiento de soporte a nivel fabricante cuando lo requiera la Dirección de Telemática de la Marina.

5.5.2.6. Deberá proporcionar alternativas de solución para no afectar la continuidad del servicio por un plazo no mayor a 72 horas.

5.5.3. Capacitación

5.5.3.1. Se podrá requerir la capacitación en administración del equipo appliance sandbox antimalware, el cual estará dirigido a un mínimo de TRES (3) técnicos de la División de Ciberseguridad de la DIRTEL, con un tiempo mínimo de duración de 8 horas, a realizarse en las instalaciones de la Entidad, o en forma virtual, dentro de los 3 meses posteriores a la culminación de las actividades tipificadas en el numeral 5.1.

5.5.3.2. El sylabus corresponderá a la versión del equipo appliance sandbox antimalware implementada y será elaborado por el proveedor en coordinación con la DIRTEL.

5.5.3.3. El material a entregar deberá contemplar el detalle de todos los temas a dictarse según el sylabus.

5.5.3.4. Se deberá otorgar constancias de participación para el personal que siga la capacitación.

5.5.4. Garantía

5.5.4.1. El proveedor presentará la garantía de buen funcionamiento será por el mismo periodo de vigencia del licenciamiento. Asimismo, iniciará al mismo tiempo que la vigencia del licenciamiento del software de seguridad implementado por el proveedor.

5.5.4.2. La garantía de buen funcionamiento comprende que la solución ofertada cumpla con todos los requerimientos tipificados en el presente documento.

5.6. Lugar y plazo de la prestación

5.6.1. Lugar

La prestación del servicio será en la Dirección de Telemática de la Marina, cito en Av. La Marina Cdra. 36 S/N, dentro de la Estación Naval La Perla.

5.6.2. Plazo

5.6.2.1. El plazo para la configuración del servicio del periodo comprendido entre el años 2021 - 2022, será de 50 días calendario, contabilizados a partir del día siguiente de la firma del contrato.

5.6.2.2. La configuración del servicio del periodo comprendido entre el años 2022 – 2023 y 2023 - 2024, será de máximo 10 días calendarios antes de la caducidad de la licencia vigente.

5.6.2.3. El plazo de ejecución del servicio es de 1,095 días calendarios, dividido en tres periodos de 365 días calendarios entre los años 2021 y 2024, los mismos que corresponden a la duración del licenciamiento anual a ser espedidas.

5.7. Confidencialidad

El POSTOR deberá firmar el Acta de Confidencialidad proporcionado por la Dirección de Telemática de la Marina, para el desarrollo de los trabajos de soporte técnico y otros que se

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

realicen sobre los sistemas informáticos de la Institución, el cual se realizará a la firma del contrato.

El acuerdo de confidencialidad formará parte del contrato a fin de permitir y resguardar la Información clasificada de la Institución, pudiéndose limitar el acceso de profesionales que puedan afectar a la seguridad de la Institución.

5.8. Medidas de control durante la ejecución contractual

5.8.1. Designación de responsabilidades

5.8.1.1. Áreas que coordinarán con el proveedor: La Jefatura del Departamento de Administración de Redes y Ciberseguridad y la División de Ciberseguridad.

5.8.1.2. Área responsable de las medidas de control: La Jefatura del Departamento de Administración de Redes y Ciberseguridad.

5.8.1.3. Área que brindará la conformidad: La Jefatura de la División de Ciberseguridad.

5.8.2. Medidas de control

5.8.2.1. Supervisará que el proveedor cumpla con todo lo requerido en el presente documento.

5.8.2.2. Verificará la correcta confección del Acta de Conformidad.

5.8.3. Conformidad

Se elaborarán Actas de Conformidad en forma anual, posterior a la configuración del servicio de licenciamiento requerido, debiendo contener los siguientes documentos:

5.8.3.1. Screenshot del portal oficial del fabricante donde figuren las claves u otros indicadores que permita validar la licencia proporcionada.

5.8.3.2. Informe elaborado por el proveedor donde acredite el cumplimiento de lo tipificado en el numeral 5.1.

5.8.3.3. Declaración jurada del proveedor en el cual se compromete a brindar el mantenimiento preventivo, soporte técnico, capacitación y garantía de buen funcionamiento, de acuerdo a lo tipificado del numeral 5.5.1 al numeral 5.5.4. En dicho documento el proveedor deberá indicar los teléfonos y correos electrónicos para contacto.

5.9. Forma de pago

El pago se realizará en TRES (03) armadas, previa presentación del acta de conformidad detallada en el numeral 5.9.3, de acuerdo a lo siguiente:

5.9.1. El primer pago se efectuará en el año 2021 y corresponderá al 33.33% del monto contractual.

5.9.2. El segundo pago se efectuará en el año 2022 y corresponderá al 33.33% del monto contractual.

5.9.3. El segundo pago se efectuará en el año 2023 y corresponderá al 33.34% del monto contractual.

Importante

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

3.2. REQUISITOS DE CALIFICACIÓN

A	**CAPACIDAD LEGAL**
	HABILITACIÓN
	ÍTEM 1
	• Requisitos: El proveedor deberá ser distribuidor oficial y/o partner de la marca del producto para la solución ofertada. • El postor deberá presentar: Copia simple de la carta del fabricante que acredite que el postor es distribuidor oficial y/o partner. • En adición, 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. Promesa de consorcio con firmas legalizadas[12], en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. **(Anexo N° 5)** La promesa de consorcio debe ser suscrita por cada uno de sus integrantes. El representante común del consorcio se encuentra facultado para actuar en nombre y representación del mismo en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato, con amplias y suficientes facultades.
	ÍTEM 2 • Requisitos: El proveedor deberá ser distribuidor oficial y/o partner de la marca del producto para la solución ofertada. • El postor deberá presentar: Copia simple de la carta del fabricante que acredite que el postor es distribuidor oficial y/o partner. • En adición, 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.

[12] En caso de presentarse en consorcio.

	Promesa de consorcio con firmas legalizadas[13], en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. **(Anexo N° 5)** La promesa de consorcio debe ser suscrita por cada uno de sus integrantes. El representante común del consorcio se encuentra facultado para actuar en nombre y representación del mismo en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato, con amplias y suficientes facultades.
	ÍTEM 3 • Requisitos: El proveedor deberá ser distribuidor oficial y/o partner de la marca del producto para la solución ofertada. • El postor deberá presentar: Copia simple de la carta del fabricante que acredite que el postor es distribuidor oficial y/o partner. • En adición, 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. Promesa de consorcio con firmas legalizadas[14], en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. **(Anexo N° 5)** La promesa de consorcio debe ser suscrita por cada uno de sus integrantes. El representante común del consorcio se encuentra facultado para actuar en nombre y representación del mismo en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato, con amplias y suficientes facultades.
	ÍTEM 4 • Requisitos: El proveedor deberá ser distribuidor oficial y/o partner de la marca del producto para la solución ofertada. • El postor deberá presentar: Copia simple de la carta del fabricante que acredite que el postor es distribuidor oficial y/o partner. • En adición, 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. Promesa de consorcio con firmas legalizadas[15], en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete

[13] En caso de presentarse en consorcio.
[14] En caso de presentarse en consorcio.
[15] En caso de presentarse en consorcio.

	cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. **(Anexo N° 5)** La promesa de consorcio debe ser suscrita por cada uno de sus integrantes. El representante común del consorcio se encuentra facultado para actuar en nombre y representación del mismo en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato, con amplias y suficientes facultades. **ÍTEM 5** • Requisitos: El proveedor deberá ser distribuidor oficial y/o partner de la marca del producto para la solución ofertada. • El postor deberá presentar: Copia simple de la carta del fabricante que acredite que el postor es distribuidor oficial y/o partner. • En adición, 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. Promesa de consorcio con firmas legalizadas[16], en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. **(Anexo N° 5)** La promesa de consorcio debe ser suscrita por cada uno de sus integrantes. El representante común del consorcio se encuentra facultado para actuar en nombre y representación del mismo en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato, con amplias y suficientes facultades. **ÍTEM 6** • Requisitos: El proveedor deberá ser distribuidor oficial y/o partner de la marca del producto para la solución ofertada. • El postor deberá presentar: Copia simple de la carta del fabricante que acredite que el postor es distribuidor oficial y/o partner. • En adición, 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. Promesa de consorcio con firmas legalizadas[17], en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete

[16] En caso de presentarse en consorcio.
[17] En caso de presentarse en consorcio.

	cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. **(Anexo N° 5)** La promesa de consorcio debe ser suscrita por cada uno de sus integrantes. El representante común del consorcio se encuentra facultado para actuar en nombre y representación del mismo en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato, con amplias y suficientes facultades.
B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.1	**CALIFICACIONES DEL PERSONAL CLAVE**
B.3.1	**FORMACIÓN ACADÉMICA**
	ÍTEM 1 1.- UN (1) ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN Requisitos: Un Ingeniero Titulado y Colegiado en Ingeniería de Electrónica, Informática, Telecomunicaciones y/o Sistemas. Acreditación: Se acreditará presentando copia simple de título profesional a nombre de la nación y copia simple de la constancia de habilitación emitida por el colegio de ingenieros. 2.- UN (1) ESPECIALISTA RESPONSABLES DEL SOPORTE TÉCNICO Requisitos: Ingeniero Titulado o Bachiller en Ingeniería de Electrónica, Informática, Seguridad y Auditoria Informática, Redes y Comunicaciones, Telecomunicaciones, Industrial y/o Sistemas. Acreditación: Se acreditará presentando copia simple de título profesional o grado académico a nombre de la nación donde se acredite el nivel académico. El título profesional será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: http://www.titulosinstitutos.pe/, según corresponda. En caso el título profesional requerido 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. ÍTEM 2 1. UN (1) ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN Requisitos:

Un Ingeniero Titulado y Colegiado en Ingeniería de Electrónica, Informática y/o Sistemas.

Acreditación:
Se acreditará presentando copia simple de título profesional a nombre de la nación y copia simple de la constancia de habilitación emitida por el colegio de ingenieros.

2. DOS (2) ESPECIALISTAS RESPONSABLES DEL SOPORTE TÉCNICO

Requisitos:
Ingenieros Titulados en Ingeniería de Electrónica, Informática, Seguridad y Auditoria Informática, Redes y Comunicaciones, Industrial y/o Sistemas.

Acreditación:

Presentar copia simple del título profesional a nombre de la nación donde se acredite el nivel académico.

El título profesional será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: http://www.titulosinstitutos.pe/, según corresponda.

En caso el título profesional requerido 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.

ÍTEM 3

1. UN (1) ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN

Requisitos:
Un Ingeniero Titulado y Colegiado en Ingeniería de Electrónica, Informática y/o Sistemas.

Acreditación:
Se acreditará presentando copia simple de título profesional a nombre de la nación y copia simple de la constancia de habilitación emitida por el colegio de ingenieros.

2. DOS (2) ESPECIALISTAS RESPONSABLES DEL SOPORTE TÉCNICO

Requisitos:
Ingenieros Titulados y/o Bachilleres en Ingeniería de Electrónica, Informática, Seguridad y Auditoria Informática, Telecomunicaciones y/o Sistemas.

Acreditación:
Se acreditará presentando copia simple de título profesional a nombre de la nación donde se acredite el nivel académico.

El título profesional será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: http://www.titulosinstitutos.pe/, según corresponda.

En caso el título profesional requerido 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.

ÍTEM 4

1. UN (1) ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN

Requisitos:
Un Ingeniero Titulado y Colegiado en Ingeniería de Electrónica, Informática y/o Sistemas.

Acreditación:
Se acreditará presentando copia simple de título profesional a nombre de la nación y copia simple de la constancia de habilitación emitida por el colegio de ingenieros.

2. TRES (3) ESPECIALISTAS RESPONSABLES DEL SOPORTE TÉCNICO

Requisitos:
Ingenieros Titulados y/o Bachilleres en Ingeniería de Electrónica, Informática, Seguridad y Auditoria Informática, Telecomunicaciones y/o Sistemas.

Acreditación:
Se acreditará presentando copia simple de título profesional a nombre de la nación donde se acredite el nivel académico.

El título profesional será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: http://www.titulosinstitutos.pe/, según corresponda.

En caso el título profesional requerido 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.

ÍTEM 5

1. UN (1) ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN

Requisitos:
Un Ingeniero Titulado y Colegiado en Ingeniería de Electrónica, Informática y/o Sistemas.

Acreditación:
Se acreditará presentando copia simple de título profesional a nombre de la nación y copia simple de la constancia de habilitación emitida por el colegio de ingenieros.

2. UN (1) ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN

Requisitos:
Ingenieros Titulados en Ingeniería de Electrónica, Informática, Seguridad y Auditoria Informática, Redes y Comunicaciones, Industrial y/o Sistemas.

Acreditación:
Se acreditará presentando copia simple de título profesional a nombre de la nación donde se acredite el nivel académico.

El título profesional será verificado por el comité de selección en el Registro Nacional

	de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: http://www.titulosinstitutos.pe/, según corresponda. En caso el título profesional requerido 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. ÍTEM 6 1. UN (1) ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN Requisitos: Un Ingeniero Titulado y Colegiado en Ingeniería de Electrónica, Informática, Telecomunicaciones y/o Sistemas. Acreditación: Se acreditará presentando copia simple de título profesional a nombre de la nación y copia simple de la constancia de habilitación emitida por el colegio de ingenieros. 2. UN (1) ESPECIALISTA RESPONSABLES DEL SOPORTE TÉCNICO Requisitos: Ingeniero Titulado o Bachiller en Ingeniería de Electrónica, Informática, Seguridad y Auditoria Informática, Redes y Comunicaciones, Telecomunicaciones, Industrial y/o Sistemas. Acreditación: Se acreditará presentando copia simple de título profesional a nombre de la nación donde se acredite el nivel académico. El título profesional será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe/ // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: http://www.titulosinstitutos.pe/, según corresponda. En caso el título profesional requerido 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**
	ÍTEM 1 1. ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN Requisitos: Debe encontrarse certificado en CheckPoint Certified Administrator o Profesional de Seguridad de Red vigente respecto a la solución a implementar. Debe encontrarse certificado en Administración de la Consola de Reportes vigente respecto a la solución a implementar.

	Debe encontrarse certificado en Profesional de IPv6 vigente emitido por una Backbone global en Internet (ISP). Debe encontrarse certificado en la Herramienta de Análisis de Vulnerabilidades utilizada durante el primer mantenimiento preventivo. Acreditación: Copia simple de constancias, certificados u otros documentos, según corresponda. 2. ESPECIALISTA RESPONSABLES DEL SOPORTE TÉCNICO Requisitos: Debe encontrarse certificado en CheckPoint Certified Administrator o Profesional de Seguridad de Red vigente respecto a la solución a implementar. De encontrarse certificado como Auditor Líder ISO 27001 emitido por entidad certificadora oficial. Debe encontrarse certificado en Profesional de IPv6 vigente emitido por una Backbone global en Internet (ISP). Debe encontrarse certificados en la Herramienta de Análisis de Vulnerabilidades a ser utilizado cuando lo requiera la DIRTEL. Acreditación: Copia simple de constancias, certificados u otros documentos, según corresponda. ÍTEM 2 1. ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN Requisitos: Debe estar certificado de entrenamiento oficial en Administración de Firewall de Aplicaciones Web emitido por el fabricante de la solución ofertada Debe encontrarse certificado como Especialista de Seguridad Web emitido por fabricante de Soluciones de Seguridad Web Debe tener certificación ITIL o ISO/IEC 20000 para la gestión de Servicios vigente emitido por empresa certificadora autorizada. Debe tener certificación vigente ISO 9001 para la gestión de la Calidad emitido por empresa certificadora autorizada. Debe encontrarse certificado en Ethical Hacking vigente emitido por Mile2 o ECCouncil. Debe encontrarse certificado en Fundamentos de Ciberseguridad vigente emitido por una empresa certificadora autorizada. Debe encontrarse certificado en Fundamentos de Continuidad de Negocio vigente emitido por una empresa certificadora autorizada. Debe encontrarse certificado en la Herramienta de Análisis de Vulnerabilidades utilizada durante el primer mantenimiento preventivo. Deben encontrarse certificado en Profesional de IPv6 vigente emitido por una Backbone global en Internet (ISP). Acreditación: Copia simple de constancias, certificados u otros documentos, según corresponda. 2. ESPECIALISTAS RESPONSABLES DEL SOPORTE TÉCNICO Requisitos: Deben tener certificado de entrenamiento oficial en Administración de Firewall de Aplicaciones Web emitido por el fabricante de la solución ofertada. Deben tener certificación ITIL o ISO/IEC 20000 para la gestión de Servicios vigente emitido por empresa certificadora autorizada. Deben tener certificación vigente ISO 9001 e ISO/IEC 27001 Fundamentos o Asociado emitido por empresa certificadora autorizada.

Al menos uno de ellos deberá tener certificación CISSP emitido por una empresa certificadora autorizada.
Al menos uno de ellos deberá tener certificación CCIE emitido por una empresa certificadora autorizada.
Deben encontrarse certificado en la Herramienta de Análisis de Vulnerabilidades a ser utilizada cuando se requiera.
Deben encontrarse certificado en Profesional de IPv6 vigente emitido por una Backbone global en Internet (ISP).

Acreditación:
Copia simple de constancias, certificados u otros documentos, según corresponda.

ÍTEM 3

1. ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN

Requisitos:
Debe encontrarse certificado en Administración de Seguridad Web vigente emitido por una empresa certificadora autorizada.
Debe encontrarse certificado en Ethical Hacking vigente emitido por Mile2 o ECCouncil.
Debe encontrarse certificado en Fundamentos de Ciberseguridad vigente emitido por una empresa certificadora autorizada.
Debe encontrarse certificado en Fundamentos de Continuidad de Negocio vigente emitido por una empresa certificadora autorizada.
Debe encontrarse certificado en la Herramienta de Análisis de Vulnerabilidades utilizada durante el primer mantenimiento preventivo.

Acreditación:
Copia simple de constancias, certificados u otros documentos, según corresponda.

2. ESPECIALISTAS RESPONSABLES DEL SOPORTE TÉCNICO

Requisitos:
Deben encontrarse certificado en Administración de Seguridad Web vigente emitido por una empresa certificadora autorizada.
Deben encontrarse certificado en Profesional de IPv6 vigente emitido por una Backbone global en Internet (ISP).
Deben encontrarse certificados en la Herramienta de Análisis de Vulnerabilidades utilizada durante el primer mantenimiento preventivo.
Al menos uno de ellos deberá encontrarse certificado como Auditor ISO 27001 vigente emitido por una empresa certificadora autorizada
Al menos uno de ellos deberá encontrarse certificado en CISSP vigente emitido por una empresa certificadora autorizada emitido por una empresa certificadora autorizada.

Acreditación:
Copia simple de constancias, certificados u otros documentos, según corresponda.

ÍTEM 4

1. ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN

Requisitos:
Debe encontrarse certificado Profesional en Seguridad y Administración de Seguridad Endpoint vigente emitido por el fabricante de la solución ofertada.
Debe encontrarse certificado en Ethical Hacking vigente emitido por Mile2 o ECCouncil.

Debe encontrarse certificado en Fundamentos de Ciberseguridad vigente emitido por una empresa certificadora autorizada.
Debe encontrarse certificado en Fundamentos de Continuidad de Negocio vigente emitido por una empresa certificadora autorizada.
Debe encontrarse certificado en la Herramienta de Análisis de Vulnerabilidades utilizada durante el primer mantenimiento preventivo.

Acreditación:
Copia simple de constancias, certificados u otros documentos, según corresponda.

2. ESPECIALISTAS RESPONSABLES DEL SOPORTE TÉCNICO

Requisitos:
Deben encontrarse certificados a nivel Profesional en Seguridad y Administración de Seguridad Endpoint vigente emitido por el fabricante de la solución ofertada.
Deben encontrarse certificado en Profesional de IPv6 vigente emitido por una Backbone global en Internet (ISP).
Deben encontrarse certificados en la Herramienta de Análisis de Vulnerabilidades utilizada durante el primer mantenimiento preventivo.
Al menos uno de ellos deberá encontrarse certificado en Auditor ISO 27001 vigente emitido por una empresa certificadora autorizada
Al menos uno de ellos deberá encontrarse certificado en CISSP vigente emitido por una empresa certificadora autorizada

Acreditación:
Copia simple de constancias, certificados u otros documentos, según corresponda.

ÍTEM 5

1. ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN

Requisitos:
Debe encontrarse certificado en firewall de apliaciones web emitido por el fabricante de la solución ofertada
Debe tener certificación ITIL o ISO/IEC 20000 para la Gestión de Servicios vigente emitido por empresa certificadora autorizada.
Debe tener certificación vigente ISO 9001 para la gestión de la Calidad e ISO/IEC 27001 emitido por empresa certificadora autorizada.
Debe encontrarse certificado en Ethical Hacking vigente emitido por Mile2 o ECCouncil.
Debe encontrarse certificado en Fundamentos de Ciberseguridad vigente emitido por una empresa certificadora autorizada.
Debe encontrarse certificado en Fundamentos de Continuidad de Negocio vigente emitido por una empresa certificadora autorizada.
Debe encontrarse certificado en la Herramienta de Análisis de Vulnerabilidades utilizada durante el primer mantenimiento preventivo.
Debe encontrarse certificado en Profesional de IPv6 vigente emitido por una Backbone global en Internet (ISP).

Acreditación:
Copia simple de constancias, certificados u otros documentos, según corresponda.

2. ESPECIALISTA RESPONSABLE DEL SOPORTE TÉCNICO

Requisitos:
Debe encontrarse certificado en Firewall de Base de Datos emitido por el fabricante de Seguridad de Base de Datos.
Debe tener certificación ITIL o ISO/IEC 20000 para la gestión de Servicios vigente emitido por empresa certificadora autorizada.

	Debe haber llevado entrenamiento oficial en Administración de Base de Datos Microsoft SQL Server. Debe haber llevado Diplomado en Seguridad de la Información con duración mínima de 200 horas en Institución Educativa Universitaria. Debe encontrarse certificado en la Herramienta de Análisis de Vulnerabilidades utilizada durante el primer mantenimiento preventivo. Deben encontrarse certificado en Profesional de IPv6 vigente emitido por una Backbone global en Internet (ISP). Acreditación: Copia simple de constancias, certificados u otros documentos, según corresponda. ÍTEM 6 1. ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN Requisitos: Debe encontrarse certificado en CheckPoint Certified Administrator o Profesional de Seguridad de Red vigente respecto a la solución a implementar. Debe encontrarse certificado en Administración de la Consola de Reportes vigente respecto a la solución a implementar. Deben encontrarse certificado en Profesional de IPv6 vigente emitido por una Backbone global en Internet (ISP). Debe encontrarse certificado en la Herramienta de Análisis de Vulnerabilidades utilizada durante el primer mantenimiento preventivo. Acreditación: Copia simple de constancias, certificados u otros documentos, según corresponda. 2. ESPECIALISTA RESPONSABLES DEL SOPORTE TÉCNICO Requisitos: Debe encontrarse certificado en CheckPoint Certified Administrator o Profesional de Seguridad de Red vigente respecto a la solución a implementar. Debe encontrarse certificado como Auditor Lider ISO 27001 emitido por entidad certificadora oficial. Debe encontrarse certificado en Profesional de IPv6 vigente emitido por una Backbone global en Internet (ISP). Debe encontrarse certificados en la Herramienta de Análisis de Vulnerabilidades a ser utilizado cuando lo requiera la DIRTEL. Acreditación: Copia simple de constancias, certificados u otros documentos, según corresponda. **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** ÍTEM 1 1. ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN Requisitos: La persona a desempeñarse como especialista responsable de la Implementación tendrá experiencia de por lo menos TRES (03) años en instalación, administración y soporte técnico en soluciones de seguridad perimetral.

	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. 2. DOS (2) ESPECIALISTAS RESPONSABLES DEL SOPORTE TÉCNICO Requisitos: Las personas para desempeñarse como especialista responsable del soporte técnico tendrán experiencia de por lo menos DOS (02) años en la instalación y configuración de soluciones de seguridad perimetral. 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. ÍTEM 2 1. ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN Requisitos: La persona a desempeñarse como especialista responsable de la Implementación tendrá experiencia de por lo menos TRES (03) años en instalación, administración y soporte técnico de la solución de seguridad de aplicaciones web. 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. 2. DOS (2) ESPECIALISTAS RESPONSABLES DEL SOPORTE TÉCNICO Requisitos: Las personas para desempeñarse como especialista responsable del soporte técnico tendrán experiencia de por lo menos TRES (03) años en la instalación y configuración de soluciones de seguridad de aplicaciones web. 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. ÍTEM 3 1. ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN Requisitos: La persona a desempeñarse como especialista responsable de la Implementación tendrá experiencia de por lo menos TRES (03) años en instalación, administración y soporte técnico de la solución de seguridad de filtro de contenido web.

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.

2. DOS (2) ESPECIALISTAS RESPONSABLES DEL SOPORTE TÉCNICO

Requisitos:
Las personas para desempeñarse como especialista responsable del soporte técnico tendrán experiencia de por lo menos TRES (03) años en la Instalación y configuración de soluciones de seguridad de filtro de contenido web.

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.

ÍTEM 4

1. ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN

Requisitos:
La persona a desempeñarse como especialista responsable de la Implementación tendrá experiencia de por lo menos TRES (03) años en instalación, administración y soporte técnico de soluciones endpoint.

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.

2. TRES (3) ESPECIALISTAS RESPONSABLES DEL SOPORTE TÉCNICO

Requisitos:
Las personas para desempeñarse como especialista responsable del soporte técnico tendrán experiencia de por lo menos TRES (03) años en la Instalación y configuración de soluciones endpoint.

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.

ÍTEM 5

1. ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN

Requisitos:
La persona a desempeñarse como especialista responsable de la Implementación tendrá experiencia de por lo menos TRES (03) años en instalación, administración y soporte técnico de la solución de seguridad de base datos.

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

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.

2. ESPECIALISTA RESPONSABLE DEL SOPORTE TÉCNICO

Requisitos:
Las personas para desempeñarse como especialista responsable del soporte técnico tendrán experiencia de por lo menos TRES (03) años en la Instalación y configuración de soluciones de seguridad de base de datos.

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.

ÍTEM 6

1. ESPECIALISTA RESPONSABLE DE LA IMPLEMENTACIÓN

Requisitos:
La persona a desempeñarse como especialista responsable de la Implementación tendrá experiencia de por lo menos TRES (03) años en instalación, administración y soporte técnico en soluciones de seguridad perimetral.

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.

2. DOS (2) ESPECIALISTAS RESPONSABLES DEL SOPORTE TÉCNICO

Requisitos:
Las personas para desempeñarse como especialista responsable del soporte técnico tendrán experiencia de por lo menos DOS (02) años en la Instalación y configuración de soluciones de seguridad perimetral.

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 documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la Entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.*** • ***En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.*** • ***Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.*** • ***Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.***
C	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**
	ÍTEM 1 Requisitos: Monto facturado acumulado por UN MILLÓN CON 00/100 SOLES (S/1'000,000.00) por la contratación de servicios iguales o similares al objeto de la convocatoria. Se considerarán servicios iguales o similares los siguientes: venta y renovación de licencias y/o equipos de seguridad informática y/o renovación de soporte o mantenimiento de equipos de seguridad informática, 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. 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 [18], correspondientes a un máximo de veinte (20) contrataciones.

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

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

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

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

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

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

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

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

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

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

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

ÍTEM 2

Requisitos:

Monto facturado acumulado por SETECIENTOS MIL CON 00/100 (S/ 700,000.00) por la contratación de servicios iguales o similares al objeto de la convocatoria. Se considerarán servicios iguales o similares los siguientes: venta y renovación de licencias y/o equipos de seguridad informática y/o renovación de soporte o mantenimiento de equipos de seguridad informática, 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.

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 [19], correspondientes a un máximo de veinte (20) contrataciones.

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

En el caso de 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 una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9.**

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

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

[19] 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".

ÍTEM 3

Requisitos:

Monto facturado acumulado por SEISCIENTOS MIL CON 00/100 SOLES (S/ 600,000.00) por la contratación de servicios iguales o similares al objeto de la convocatoria. Se considerarán servicios iguales o similares los siguientes: venta y renovación de licencias y/o equipos de seguridad informática y/o renovación de soporte o mantenimiento de equipos de seguridad informática, 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.

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 [20], correspondientes a un máximo de veinte (20) contrataciones.

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

En el caso de 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,

[20] 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".

debiendo acompañar la documentación sustentatoria correspondiente.

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

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

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

ÍTEM 4

Requisitos:

Monto facturado acumulado por SEISCIENTOS MIL CON 00/100 (S/ 600,000.00) por la contratación de servicios iguales o similares al objeto de la convocatoria. Se considerarán servicios iguales o similares los siguientes: venta y renovación de licencias y/o equipos de seguridad informática y/o renovación de soporte o mantenimiento de equipos de seguridad informática, 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.

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 [21], correspondientes a un máximo de veinte (20) contrataciones.

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

En el caso de 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

[21] 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".

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

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

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

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

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

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

ÍTEM 5

Requisitos:

Monto facturado acumulado por SETECIENTOS MIL CON 00/100 (S/ 700,000.00) por la contratación de servicios iguales o similares al objeto de la convocatoria. Se considerarán servicios iguales o similares los siguientes: venta y renovación de licencias y/o equipos de seguridad informática y/o renovación de soporte o mantenimiento de equipos de seguridad informática, 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.

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 [22], correspondientes a un máximo de veinte (20)

[22] 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".

contrataciones.

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

En el caso de 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 una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9.**

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

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

ÍTEM 6

Requisitos:

Monto facturado acumulado por CUATROCIENTOS MIL CON 00/100 SOLES (S/ 400,000.00) por la contratación de servicios iguales o similares al objeto de la convocatoria. Se considerarán servicios iguales o similares los siguientes: venta y renovación de licencias y/o equipos de seguridad informática y/o renovación de soporte o mantenimiento de equipos de seguridad informática, 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.

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 [23], correspondientes a un máximo de veinte (20) contrataciones.

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

En el caso de 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 una persona absorbida como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9.**

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

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

[23] 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.*

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

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 registro en el SEACE o el documento que contiene el precio de la oferta **(Anexo N° 6)**, según corresponda.	La evaluación consistirá en otorgar el máximo puntaje a la oferta de precio más bajo y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos precios, según la siguiente fórmula: $Pi = \frac{Om \times PMP}{Oi}$ i= Oferta Pi= Puntaje de la oferta a evaluar Oi=Precio i Om= Precio de la oferta más baja PMP=Puntaje máximo del precio **100 puntos**

Importante

Los factores de evaluación elaborados por el órgano encargado de las contrataciones o el comité de selección, según corresponda, son objetivos y guardan vinculación, razonabilidad y proporcionalidad con el objeto de la contratación. Asimismo, estos no pueden calificar con puntaje el cumplimiento de 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[CONSIGNAR LA DENOMINACIÓN DE LA CONVOCATORIA], que celebra de una parte [CONSIGNAR EL NOMBRE DE LA ENTIDAD], en adelante LA ENTIDAD, con RUC N° [.....], con domicilio legal en [.....], representada por [.....], identificado con DNI N° [.....], y de otra parte [.....], con RUC N° [.....], con domicilio legal en [.....], inscrita en la Ficha N° [.....] Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], debidamente representado por su Representante Legal, [.....], con DNI N° [.....], según poder inscrito en la Ficha N° [.....], Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES
Con fecha [.....], el órgano encargado de las contrataciones o el comité de selección, según corresponda, adjudicó la buena pro de la **ADJUDICACIÓN SIMPLIFICADA N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO DE SELECCIÓN]** para la contratación de [CONSIGNAR LA DENOMINACIÓN DE LA CONVOCATORIA], a [INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO], cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO
El presente contrato tiene por objeto [CONSIGNAR EL OBJETO DE LA CONTRATACIÓN].

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[24]
LA ENTIDAD se obliga a pagar la contraprestación a EL CONTRATISTA en [INDICAR MONEDA], en [INDICAR SI SE TRATA DE PAGO ÚNICO, PAGOS PARCIALES O PAGOS PERIÓDICOS], luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 171 del Reglamento de la Ley de Contrataciones del Estado.

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

LA ENTIDAD debe efectuar el pago dentro de los diez (10) días calendario siguientes de otorgada

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

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 [.....], el mismo que se computa desde [CONSIGNAR SI ES DEL DÍA SIGUIENTE DEL PERFECCIONAMIENTO DEL CONTRATO, 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].

Importante para la Entidad

De preverse en los Términos de Referencia la ejecución de actividades de instalación, implementación u otros que deban realizarse de manera previa al inicio del plazo de ejecución, se debe consignar lo siguiente:
"El plazo para la [CONSIGNAR LAS ACTIVIDADES PREVIAS PREVISTAS EN LOS TÉRMINOS DE REFERENCIA] *es de* [.....], *el mismo que se computa desde* [INDICAR CONDICIÓN CON LA QUE DICHAS ACTIVIDADES SE INICIAN]."

Incorporar a las bases o eliminar, según corresponda.

Importante para la Entidad

En el caso de contratación de prestaciones accesorias, se puede incluir la siguiente cláusula:

CLÁUSULA ...: PRESTACIONES ACCESORIAS[25]

"Las prestaciones accesorias tienen por objeto [CONSIGNAR EL OBJETO DE LAS PRESTACIONES ACCESORIAS].

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

El plazo de ejecución de las prestaciones accesorias es de [.....], el mismo que se computa desde [CONSIGNAR SI ES DEL DÍA SIGUIENTE DEL CUMPLIMIENTO DE LAS PRESTACIONES PRINCIPALES, 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 DE LAS PRESTACIONES ACCESORIAS, DEBIENDO INDICAR LAS MISMAS EN ESTE ULTIMO CASO].

[DE SER EL CASO, INCLUIR OTROS ASPECTOS RELACIONADOS A LA EJECUCIÓN DE LAS PRESTACIONES ACCESORIAS]."

Incorporar a las bases o eliminar, según corresponda

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,

[25] De conformidad con la Directiva sobre prestaciones accesorias, los contratos relativos al cumplimiento de la(s) prestación(es) principal(es) y de la(s) prestación(es) accesoria(s), pueden estar contenidos en uno o dos documentos. En el supuesto que ambas prestaciones estén contenidas en un mismo documento, estas deben estar claramente diferenciadas, debiendo indicarse entre otros aspectos, el precio y plazo de cada prestación.

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."*

En el caso que corresponda, consignar lo siguiente:

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

Importante

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

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

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

Importante para la Entidad

Sólo en el caso que la Entidad hubiese previsto otorgar adelanto, se debe incluir la siguiente cláusula:

CLÁUSULA NOVENA: ADELANTO DIRECTO

"LA ENTIDAD otorgará [CONSIGNAR NÚMERO DE ADELANTOS A OTORGARSE] *adelantos directos por el* [CONSIGNAR PORCENTAJE QUE NO DEBE EXCEDER DEL 30% DEL MONTO DEL CONTRATO ORIGINAL] *del monto del contrato original.*

EL CONTRATISTA debe solicitar los adelantos dentro de [CONSIGNAR EL PLAZO Y OPORTUNIDAD PARA LA SOLICITUD]*, adjuntando a su solicitud la garantía por adelantos mediante* [INDICAR TIPO DE GARANTÍA, CARTA FIANZA Y/O PÓLIZA DE CAUCIÓN] *acompañada del comprobante de pago correspondiente. Vencido dicho plazo no procederá la solicitud.*

LA ENTIDAD debe entregar el monto solicitado dentro de [CONSIGNAR EL PLAZO] *siguientes a la presentación de la solicitud del contratista."*

Incorporar a las bases o eliminar, según corresponda.

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 [CONSIGNAR EL ÁREA O UNIDAD ORGÁNICA QUE OTORGARÁ LA CONFORMIDAD] 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 [CONSIGNAR TIEMPO EN AÑOS, NO MENOR DE UN (1) AÑO] año(s) contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DÉCIMA TERCERA: PENALIDADES

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

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

Donde:

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

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

Importante

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

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

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

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

CLÁUSULA DÉCIMA CUARTA: RESOLUCIÓN DEL CONTRATO

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

CLÁUSULA DÉCIMA QUINTA: RESPONSABILIDAD DE LAS PARTES

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

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

CLÁUSULA DÉCIMA SEXTA: ANTICORRUPCIÓN

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

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

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

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[26]

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

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

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

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

CLÁUSULA DÉCIMA NOVENA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

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

CLÁUSULA VIGÉSIMA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

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

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

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

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

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

"LA ENTIDAD"

"EL CONTRATISTA"

[26] 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).

ANEXOS

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 020-2021 MGP/DIRTEL
Presente.-

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

Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[27]		Sí		No	
Correo electrónico :					

Autorización de notificación por correo electrónico:

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.
4. Respuesta a la solicitud de acceso al expediente de contratación.
5. Notificación de la orden de servicios[28]

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.

[27] 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 original, en calidad de garantía de fiel cumplimiento, en los contratos periódicos de prestación de servicios, según lo señalado en el artículo 149 del Reglamento. Asimismo, dicha información se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

[28] Cuando el monto del valor estimado del procedimiento o del ítem no supere los cien mil Soles (S/ 100 000.00), en caso 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
ADJUDICACIÓN SIMPLIFICADA Nº 020-2021 MGP/DIRTEL
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[29]	Sí		No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE[30]	Sí		No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE[31]	Sí		No	
Correo electrónico :				

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

[29] 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 original, en calidad de garantía de fiel cumplimiento, según lo señalado en el artículo 149 del Reglamento. Asimismo, dicha información se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento. Para dichos efectos, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

[30] Ibídem.

[31] Ibídem.

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
3. Solicitud al postor que ocupó el segundo lugar en el orden de prelación para presentar los documentos para perfeccionar el contrato.
4. Respuesta a la solicitud de acceso al expediente de contratación.
5. Notificación de la orden de servicios[32]

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.

[32] Cuando el monto del valor estimado del procedimiento o del ítem no supere los cien mil Soles (S/ 100 000.00), en caso 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
ADJUDICACIÓN SIMPLIFICADA Nº 020-2021 MGP/DIRTEL
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. Que mi información (en caso que el postor sea persona natural) o la información de la persona jurídica que represento, registrada en el RNP se encuentra actualizada.

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

v. 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.

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

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

viii. 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
ADJUDICACIÓN SIMPLIFICADA Nº 020-2021 MGP/DIRTEL
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

ANEXO N° 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 020-2021 MGP/DIRTEL
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO N° 5

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

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 020-2021 MGP/DIRTEL
Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta a la **ADJUDICACIÓN SIMPLIFICADA N°** [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO]

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

a) Integrantes del consorcio

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

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

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

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

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

1. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] [%][33]

   [DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%][34]

   [DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

   TOTAL OBLIGACIONES 100%[35]

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

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

[35] 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.

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

Importante para la Entidad

En caso de la prestación de servicios bajo el sistema a precios unitarios incluir el siguiente anexo:

Esta nota deberá ser eliminada una vez culminada la elaboración de las bases

ANEXO N° 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 020-2021 MGP/DIRTEL
Presente.-

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

CONCEPTO	CANTIDAD	PRECIO UNITARIO	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 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 N° 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 020-2021 MGP/DIRTEL
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

MINISTERIO DE D... ISA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

ANEXO N° 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 020-2021 MGP/DIRTEL
Presente.-

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

OFERTA A PRECIOS UNITARIOS DE LOS COMPONENTES SIGUIENTES:

CONCEPTO	CANTIDAD	PRECIO UNITARIO	COSTO
Monto del componente a precios unitarios			

OFERTA A SUMA ALZADA DE LOS COMPONENTES SIGUIENTES:

CONCEPTO	PRECIO TOTAL
Monto del componente a suma alzada	

Monto total de la oferta	

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 en su oferta los precios unitarios de los componentes previstos para este sistema en el presente anexo y por un monto fijo integral de los componentes previstos a suma alzada.*
- *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 las disposiciones, según corresponda. Una vez culminada la elaboración de las bases, las notas que no se incorporen deben ser eliminadas

MINISTERIO DE DEFENSA – MARINA DE GUERRA DEL PERU
DIRECCION DE TELEMATICA DE LA MARINA
AS-020-2021 MGP/DIRTEL

ANEXO N° 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 020-2021 MGP/DIRTEL

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

CONCEPTO	OFERTA
Porcentaje ofertado[36]	%
Monto Total Ofertado	

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 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 las disposiciones, según corresponda. Una vez culminada la elaboración de las bases, las notas que no se incorporen deben ser eliminadas

[36] De conformidad con la Opinión N° 202-2016/DTN, corresponde al porcentaje del monto total a cobrar o recuperar.

ANEXO Nº 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA Nº 020-2021 MGP/DIRTEL
Presente.-

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

CONCEPTO	MONTO
(A) Honorario Fijo	
(B) Comisión de éxito[37]	
Precio de la Oferta (A) + (B)	

El precio de la oferta [CONSIGNAR LA MONEDA DE LA CONVOCATORIA] incluye todos los tributos, seguros, transporte, inspecciones, pruebas y, de ser el caso, los costos laborales conforme a la legislación vigente, así como cualquier otro concepto que pueda tener incidencia sobre el costo del 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 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 las disposiciones, según corresponda. Una vez culminada la elaboración de las bases, las notas que no se incorporen deben ser eliminadas

[37] De conformidad con la Opinión Nº 011-2017/DTN *"El postor formula su oferta contemplando un monto fijo y un monto adicional como incentivo que debe pagársele en caso consiga el resultado esperado".*

ANEXO Nº 7
DECLARACIÓN JURADA DE CUMPLIMIENTO DE CONDICIONES PARA LA APLICACIÓN DE LA EXONERACIÓN DEL IGV

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA Nº 020-2021 MGP/DIRTEL
Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento que gozo del beneficio de la exoneración del IGV previsto en la Ley Nº 27037, Ley de Promoción de la Inversión en la Amazonía, dado que cumplo con las condiciones siguientes:

1.- Que el domicilio fiscal de la empresa[38] se encuentra ubicada en la Amazonía y coincide con el lugar establecido como sede central (donde tiene su administración y lleva su contabilidad);

2.- Que la empresa se encuentra inscrita en las Oficinas Registrales de la Amazonía (exigible en caso de personas jurídicas);

3.- Que, al menos el setenta por ciento (70%) de los activos fijos de la empresa se encuentran en la Amazonía; y

4.- Que la empresa no presta servicios fuera de la Amazonía.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

Cuando se trate de consorcios, esta declaración jurada será presentada por cada uno de los integrantes del consorcio, salvo que se trate de consorcios con contabilidad independiente, en cuyo caso debe ser suscrita por el representante común, debiendo indicar su condición de consorcio con contabilidad independiente y el número de RUC del consorcio.

[38] En el artículo 1 del "Reglamento de las Disposiciones Tributarias contenidas en la Ley de Promoción de la Inversión en la Amazonía" se define como "empresa" a las "Personas naturales, sociedades conyugales, sucesiones indivisas y personas consideradas jurídicas por la Ley del Impuesto a la Renta, generadoras de rentas de tercera categoría, ubicadas en la Amazonía. Las sociedades conyugales son aquéllas que ejerzan la opción provista en el Artículo 16 de la Ley del Impuesto a la Renta."

ANEXO Nº 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA Nº 020-2021 MGP/DIRTEL
Presente.-

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

Nº	CLIENTE	OBJETO DEL CONTRATO	Nº CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [39]	FECHA DE LA CONFORMIDAD DE SER EL CASO [40]	EXPERIENCIA PROVENIENTE [41] DE:	MONEDA	IMPORTE [42]	TIPO DE CAMBIO VENTA [43]	MONTO FACTURADO ACUMULADO [44]
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
	...									
20										
	TOTAL									

[39] 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.

[40] 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.

[41] 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"*.

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

[43] 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.

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

[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
ADJUDICACIÓN SIMPLIFICADA Nº 020-2021 MGP/DIRTEL
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] absorbida 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 Nº 10

SOLICITUD DE BONIFICACIÓN DEL DIEZ POR CIENTO (10%) POR SERVICIOS PRESTADOS FUERA DE LA PROVINCIA DE LIMA Y CALLAO
(DE SER EL CASO, SOLO PRESENTAR ESTA SOLICITUD EN EL ITEM [CONSIGNAR EL N° DEL ÍTEM O ÍTEMS CUYO VALOR ESTIMADO NO SUPERA LOS DOSCIENTOS MIL SOLES (S/ 200,000.00)])

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA Nº 020-2021 MGP/DIRTEL
Presente.-

Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], solicito la asignación de la bonificación del diez por ciento (10%) sobre el puntaje total en [CONSIGNAR EL ÍTEM O ITEMS, SEGÚN CORRESPONDA, EN LOS QUE SE SOLICITA LA BONIFICACIÓN] debido a que el domicilio de mi representada se encuentra ubicado en la provincia o provincia colindante donde se ejecuta la prestación.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

- *Para asignar la bonificación, el órgano encargado de las contrataciones o comité de selección, según corresponda, verifica el domicilio consignado por el postor en el Registro Nacional de Proveedores (RNP).*
- *Para que el postor pueda acceder a la bonificación, debe cumplir con las condiciones establecidas en el literal f) del artículo 50 del Reglamento.*

Importante

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

ANEXO N° 10

SOLICITUD DE BONIFICACIÓN DEL DIEZ POR CIENTO (10%) POR SERVICIOS PRESTADOS FUERA DE LA PROVINCIA DE LIMA Y CALLAO
(DE SER EL CASO, SOLO PRESENTAR ESTA SOLICITUD EN EL ITEM [CONSIGNAR EL N° DEL ÍTEM O ÍTEMS CUYO VALOR ESTIMADO NO SUPERA LOS DOSCIENTOS MIL SOLES (S/ 200,000.00])

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 020-2021 MGP/DIRTEL
Presente.-

Mediante el presente el que se suscribe, [.....], representante común del consorcio [CONSIGNAR EL NOMBRE DEL CONSORCIO], solicito la asignación de la bonificación del diez por ciento (10%) sobre el puntaje total en [CONSIGNAR EL ÍTEM O ÍTEMS, SEGÚN CORRESPONDA, EN LOS QUE SE SOLICITA LA BONIFICACIÓN] debido a que los domicilios de todos los integrantes del consorcio se encuentran ubicados en la provincia o provincias colindantes donde se ejecuta la prestación.

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

- *Para asignar la bonificación, el órgano encargado de las contrataciones o comité de selección, según corresponda, verifica el domicilio consignado de los integrantes del consorcio, en el Registro Nacional de Proveedores (RNP).*
- *Para que un consorcio pueda acceder a la bonificación, cada uno de sus integrantes debe cumplir con las condiciones establecidas en el literal f) del artículo 50 del Reglamento.*

ANEXO N° 11

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

Señores
COMITÉ DE SELECCIÓN
ADJUDICACIÓN SIMPLIFICADA N° 020-2021 MGP/DIRTEL
Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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

ANEXO N° 12

(SE PRESENTARÁ FIRMADO PARA EL PERFECCIONAMIENTO DE CONTRATO-OBLIGATORIO)

DECLARACIÓN JURADA DE COMPROMISO ANTISOBORNO

Yo, ..., identificado con DNI....., representante legal de: ....., con RUC:....., me comprometo a conducirme 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, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas.

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

La Perla,

NOMBRES:.....
APELLIDOS:.....
DNI.:.....

ANEXO N° 13

(SE PRESENTARÁ FIRMADO PARA EL PERFECCIONAMIENTO DE CONTRATO-OBLIGATORIO)

DECLARACIÓN JURADA DE NO TENER IMPEDIMENTO PARA CONTRATAR CON EL ESTADO

Señores

De nuestra consideración:

Mediante la presente, el suscrito ....., identificado con D.N.I. N° ....., Representante Legal de la empresa ....., con R.U.C. N° ....., Declaro bajo juramento:

1. No tener impedimento para contratar con el Estado, conforme al artículo 11 de la Ley N° 30225 – Ley de Contrataciones del Estado, ni en ninguna otra causal contemplada en alguna disposición legal o reglamentaria de ser postor o contratista del Estado.
2. Contar con inscripción vigente en el Registro Nacional de Proveedores.
3. No encontrarme inhabilitado para contratar con el Estado.
4. Ser responsable de la veracidad de los documentos e información presentada en el proceso de Contratación.
5. Conocer las infracciones y sanciones establecidas en el artículo 50 de la Ley N° 30225 – Ley de Contrataciones del Estado y su Reglamento, así como en la Ley N° 27444 – Ley de Procedimiento Administrativo General.
6. No encontrarme prestando servicios laborales como personal civil y militar en la Marina de Guerra del Perú, en "situación de actividad".

La Perla,

HUELLA DIGITAL

Nombres: .....
Apellidos: .....
DNI.:.....