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

CONCURSO PÚBLICO Nº Nº003-2024-SUNASS

CONTRATACIÓN DEL "SERVICIO DE MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE CIBERATAQUES PARA SERVIDORES DE MISIÓN CRÍTICA SOC AAS (CYBER SECURITY OPERATIONS CENTER)"

DEBER DE COLABORACIÓN

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

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

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

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

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I
ETAPAS DEL PROCEDIMIENTO DE SELECCIÓN

1.1. REFERENCIAS

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

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

1.2. CONVOCATORIA

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

1.3. REGISTRO DE PARTICIPANTES

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

Importante

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

- *Los proveedores que deseen registrar su participación deben ingresar al SEACE utilizando su Certificado SEACE (usuario y contraseña). Asimismo, deben observar las instrucciones señaladas en el documento de orientación "Guía para el registro de participantes electrónico" publicado en https://www2.seace.gob.pe/.*

- *En caso los proveedores no cuenten con inscripción vigente en el RNP y/o se encuentren inhabilitados o suspendidos para ser participantes, postores y/o contratistas, el SEACE restringirá su registro, quedando a potestad de estos intentar nuevamente registrar su participación en el procedimiento de selección en cualquier otro momento, dentro del plazo establecido para dicha etapa, siempre que haya obtenido la vigencia de su inscripción o quedado sin efecto la sanción que le impuso el Tribunal de Contrataciones del Estado.*

1.4. FORMULACIÓN DE CONSULTAS Y OBSERVACIONES A LAS BASES

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

Importante

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

1.5. ABSOLUCIÓN DE CONSULTAS, OBSERVACIONES E INTEGRACIÓN DE BASES

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

Importante

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

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

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

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

Advertencia

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

Importante

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

1.7. FORMA DE PRESENTACIÓN DE OFERTAS

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

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

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

- *En caso la información contenida en los documentos escaneados que conforman la oferta no coincida con lo declarado a través del SEACE, prevalece la información declarada en los documentos escaneados.*
- *No se tomarán en cuenta las ofertas que se presenten en físico a la Entidad.*

1.8. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

Importante

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

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

1.9. EVALUACIÓN DE LAS OFERTAS

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

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

1.10. CALIFICACIÓN DE OFERTAS

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

1.11. SUBSANACIÓN DE LAS OFERTAS

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

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

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

1.12. RECHAZO DE LAS OFERTAS

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

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

1.13. OTORGAMIENTO DE LA BUENA PRO

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

1.14. CONSENTIMIENTO DE LA BUENA PRO

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

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

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

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

CAPÍTULO II
SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

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

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

Importante

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

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

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

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

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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

CAPÍTULO III
DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

Importante

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

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

3.2.3. GARANTÍA POR ADELANTO

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

3.3. REQUISITOS DE LAS GARANTÍAS

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

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

Advertencia
Los funcionarios de las Entidades no deben aceptar garantías emitidas bajo condiciones distintas a las establecidas en el presente numeral, debiendo tener en cuenta lo siguiente: *1. La clasificadora de riesgo que asigna la clasificación a la empresa que emite la garantía debe encontrarse listada en el portal web de la SBS (http://www.sbs.gob.pe/sistema-financiero/clasificadoras-de-riesgo).* *2. Se debe identificar en la página web de la clasificadora de riesgo respectiva, cuál es la clasificación vigente de la empresa que emite la garantía, considerando la vigencia a la fecha de emisión de la garantía.* *3. Para fines de lo establecido en el artículo 148 del Reglamento, la clasificación de riesgo B, incluye las clasificaciones B+ y B.* *4. Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en el portal web de la SBS, bastará que en una de ellas cumpla con la clasificación mínima establecida en el Reglamento.* *En caso exista alguna duda sobre la clasificación de riesgo asignada a la empresa emisora de la garantía, se deberá consultar a la clasificadora de riesgos respectiva.* *De otro lado, además de cumplir con el requisito referido a la clasificación de riesgo, a efectos de verificar si la empresa emisora se encuentra autorizada por la SBS para emitir garantías, debe revisarse el portal web de dicha Entidad (http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-emitir-cartas-fianza).* *Los funcionarios competentes deben verificar la autenticidad de la garantía a través de los mecanismos establecidos (consulta web, teléfono u otros) por la empresa emisora.*

3.4. EJECUCIÓN DE GARANTÍAS

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

3.5. ADELANTOS

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

3.6. PENALIDADES

3.6.1. PENALIDAD POR MORA EN LA EJECUCIÓN DE LA PRESTACIÓN

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

3.6.2. OTRAS PENALIDADES

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

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

3.7. INCUMPLIMIENTO DEL CONTRATO

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

3.8. PAGOS

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

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

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

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

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

3.9. DISPOSICIONES FINALES

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

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

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

CAPÍTULO I
GENERALIDADES

1.1. ENTIDAD CONVOCANTE

Nombre	:	Superintendencia Nacional de Servicios de Saneamiento - SUNASS
RUC Nº	:	20158219655
Domicilio legal	:	Av. Bernardo Monteagudo N° 210-216 Magdalena del Mar
Correo electrónico:	:	rquispe@sunass.gob.pe/ cumpire@sunass.gob.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del **"SERVICIO DE MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE CIBERATAQUES PARA SERVIDORES DE MISIÓN CRÍTICA SOC AAS (CYBER SECURITY OPERATIONS CENTER)".**

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante FORMATO DE APROBACIÓN DE EXPEDIENTE N° 058-2024 el 12 de diciembre del 2024.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Directamente Recaudados - RDR

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

El plazo máximo para la implementación del **P01** es de hasta 30 días calendarios, contados desde el día siguiente de suscrito el contrato, dentro del cual se suscribirá el acta de inicio del servicio.

El plazo para la ejecución del servicio es de 36 meses contabilizados desde la fecha establecida en el acta de inicio del servicio.

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, para cuyo efecto deben cancelar la suma de S/ 5,00 en el Banco de la Nación, en la cuenta corriente

N°00-000876356, y recabar las bases en Av. Bernardo Monteagudo 210-Magdalena del Mar 5to piso.

1.10. BASE LEGAL

- Ley N° 31953, de Presupuesto del Sector Público para el Año Fiscal 2024.
- Ley N° 31954, de Equilibrio Financiero del Presupuesto del Sector Público del Año Fiscal 2024.
- Ley N° 31955, Ley de Endeudamiento del Sector Publico para el Año Fiscal 2024.
- Decreto Supremo N° 082-2019-EF, que aprueba el Texto Único Ordenado de la Ley N° 30225, Ley de Contrataciones del Estado.
- Decreto Supremo N° 344-2018-EF, que aprueba el Reglamento de la Ley 30225, Ley de Contrataciones del Estado, y sus modificaciones.
- Decreto Supremo N° 004-2019-JUS, que aprueba el TUO de la Ley N° 27444 – Ley del Procedimiento administrativo General.
- Ley N° 27806, Ley de Transparencia y de Acceso a la Información Pública. Aprobada por Decreto Supremo N° 043-2003-PCM.
- Ley N° 27815, Ley del Código de Ética de la Función Pública.
- Directivas y Opiniones del OSCE.
- Código Civil.
- Directiva SUNASS: ATENCIÓN DE DENUNCIAS POR PRESUNTOS ACTOS DE CORRUPCIÓN Y OTORGAMIENTO DE MEDIDAS DE PROTECCIÓN AL DENUNCIANTE Código: GDI-ADP-DI001 (https://servicio.sunass.gob.pe/archivos/sgi/20240603175300.pdf).

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.

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

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

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

d) Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. (**Anexo Nº 3**)

---

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

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

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

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

g) El precio de la oferta en **SOLES**. Adjuntar obligatoriamente el **Anexo Nº 6.**

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

h) Presentar membresía activa en FIRST o certificado como SOC Type 2 o SOC Type 3, la membresía o certificado deberá corresponder al postor o fabricante de la solución ofertada. [5]

i) El proveedor deberá acreditar para admisión de la oferta ser representante o distribuidor autorizado de al menos una marca de la solución ofertada, adjuntando una carta del o los fabricantes haciendo referencia al proceso.

Importante

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

2.2.1.2. Documentos para acreditar los requisitos de calificación

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

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

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

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.

[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] En atención de la absolución de la consulta 74 de la empresa - ALLSAFE CORP E.I.R.L.

En esa medida, si la Entidad es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE[6] 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).

f) Domicilio para efectos de la notificación durante la ejecución del contrato.
g) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación [7] (**Anexo N° 12**).
h) Detalle de los precios unitarios del precio ofertado[8].
i) Estructura de costos[9].
j) Certificaciones solicitadas del personal clave señaladas en el numeral 9.1 de los términos de referencia.

Importante

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

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

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

Importante

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

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

[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 comprenden la oferta.

- *Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.*
- *De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya[10].*
- *La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.*

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en Mesa de Partes (de lunes a viernes en el horario de 9 am a 17:00 pm) de SUNASS, ubicada en Av. Bernardo Monteagudo 210 Magdalena del Mar, con Atención a la Unidad de Abastecimiento; o por Mesa de Partes Virtual de la SUNASS, debiendo enviar la documentación correspondiente a ésta última, la cual se encuentra ubicada en el siguiente enlace:
http://notificaciones.sunass.gob.pe:8080/mesadepartes/inicio-general

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en soles y seis (06) armadas parciales, las mismas que se distribuirán de la siguiente manera:

Pago N°	% del monto total	Condición para el pago
Primer pago	20%	Conformidad del Entregable 1
Segundo pago	16%	Conformidad del Entregable 2
Tercer pago	16%	Conformidad del Entregable 3
Cuarto pago	16%	Conformidad del Entregable 4
Quinto pago	16%	Conformidad del Entregable 5
Sexto pago	16%	Conformidad del Entregable 6

Para efectos del pago, el contratista deberá presentar sus entregables de acuerdo a lo descrito en el numeral 16.2 Presentación de Productos y Entregables de los términos de referencia, y la siguiente documentación:

-Documentación y/o contenido de cada producto según numeral 8.2.4 Elaboración de los Productos y Entregables (de los Términos de referencia).
-Comprobante de pago
-Informe técnico del Coordinador designado por la Oficina de Tecnologías de Información.
-Acta de conformidad del jefe de la Oficina de tecnologías de la Información-OTI.

El contratista deberá presentar sus entregables por mesa de partes presencial (de lunes a viernes en el horario de 9:00 a 17:00 horas) de la entidad, ubicada en Av. Bernardo Monteagudo N° 210 Magdalena del Mar o en Mesa de Partes Virtual a la siguiente dirección:
http://notificaciones.sunass.gob.pe:8080/mesadepartes/inicio-general

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

CAPÍTULO III
REQUERIMIENTO

3.1. TERMINOS DE REFERENCIA

TÉRMINOS DE REFERENCIA

1. DENOMINACIÓN DE LA CONTRATACIÓN

Contratación del "Servicio de monitoreo, prevención, detección y respuesta ante ciberataques para servidores de misión crítica SOC AAS (Cyber Security Operations Center)".

2. DEPENDENCIA SOLICITANTE

Oficina de Tecnologías de Información.

3. FINALIDAD PUBLICA

Contratar el servicio de monitoreo de ciberseguridad de los sistemas informáticos de la SUNASS mediante un Centro de Operaciones virtual de Seguridad Cibernético (Cyber Security Operations Center) el cual pueda cubrir puntos ciegos a través de capacidades de MONITOREO, PREVENCIÓN, DETECCIÓN y RESPUESTA 24x7, ante diversos tipos de ciberataques a partir del trabajo de profesionales capacitados que sostengan la gestión sobre procesos de respuesta a incidentes maduros y tecnología que permita anticiparse a los atacantes internos o externos que pudieran tener como objetivo la SUNASS.

Firmado por: CABRERA JAUREGUI Janeth Ingeborg FAU 20159219655 soft Motivo: Firma Digital Fecha: 17/01/2025 18:16:08 -0500

Firmado por: MENDEZ MONTOYA Luis Victor FAU 20159219655 soft Motivo: Firma Digital Fecha: 17/01/2025 18:29:40 -0500

Firmado por: OCHOA SURCO Arturo David FAU 20159219655 soft Motivo: Firma Digital Fecha: 17/01/2025 21:33:19 -0500

Firmado por: CALLIRGOS PAZ Jose Antonio FAU 20159219655 soft Motivo: Firma Digital Fecha: 17/01/2025 22:08:24 -0500

4. ANTECEDENTES

- La Superintendencia Nacional de Servicios de Saneamiento (SUNASS) es un organismo público regulador, creado por Decreto Ley N°25965, y adscrito a la Presidencia del Consejo de Ministros (PCM), con personería jurídica de derecho público interno y autonomía administrativa, funcional, técnica, económica y financiera. Sus funciones buscan garantizar la prestación de los servicios de saneamiento, en el ámbito urbano y rural, en condiciones de calidad, a fin de contribuir a la salud de la población y a la preservación del medioambiente.

- El servicio requerido deberá permitir la optimización de estrategias de mitigación de incidentes de seguridad cibernética, brindando las herramientas tecnológicas necesarias para la prevención, detección y respuesta ante ciberataques para servidores de misión crítica SOC AAS(Cyber Security Operations Center)".

5. OBJETIVOS DE LA CONTRATACIÓN

5.1 OBJETIVO GENERAL

Contar con el Servicio de Monitoreo y Respuesta Ante Incidentes de Seguridad Cibernética o Ciberataques que provea un servicio de seguridad holística que asegure la alerta temprana y contención oportuna ante cualquier ataque dirigido y no dirigido sobre los servidores de misión crítica de la INSTITUCIÓN.

5.2 OBJETIVOS ESPECIFICOS:

5.2.1 Proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales, efectivo permanente 24x7 por parte del servicio, documentando eventos de seguridad de múltiples fuentes en tiempo real desde una plataforma, administrada con el fin de disminuir los riesgos de ataques cibernéticos.

5.2.2 Correlacionar todos los eventos a diversas fuentes teniendo como requerimiento mínimo fuentes como el antivirus de punto final, firewall perimetral, correo electrónico, eventos del sistema, actividad de directorio activo y diversos sistemas de seguridad a fin de detectar y responder de forma oportuna ante cualquier ciber ataque y/o anomalía de seguridad.

5.2.3 ~~Revisar y atender~~ Detectar, analizar y tomar acción oportunamente ante las posibles amenazas cibernéticas de manera automática (menos de 1 minuto) a la que la INSTITUCIÓN está expuesta, relacionando vulnerabilidades, configuraciones débiles e información comprometida en la dark web.

5.2.4 Identificar vulnerabilidades de la red de datos de la INSTITUCIÓN con el fin de implementar posibles contingencias.

5.2.5 Contener cualquier tipo de ataque a través del aislamiento de un equipo y/o servidor afectado de manera automatizada, sin intervención humana.

5.2.6 Construir una mejor postura de seguridad en el tiempo basados en la evidencia que generan los eventos y amenazas identificadas por el servicio, diseñando un plan de acción para cada oportunidad de mejora.

6 VINCULACIÓN POI

"Elaboración de instrumentos estratégicos en tecnologías de la información".

7 FUENTE DE FINANCIAMIENTO

Recursos Directamente Recaudados (RDR).

8 ALCANCE Y DESCRIPCIÓN DEL SERVICIO

8.1 ALCANCE DEL SERVICIO

El servicio deberá brindar capacidades de prevención, detección, y respuesta oportuna automatizada e inmediata (menos de 1 minuto) a cualquier tipo de ciberataques delegando íntegramente la responsabilidad de la ciberseguridad de la INSTITUCIÓN al contratista del SOC distribuidos estratégicamente entre BLUE TEAM[1], RED TEAM[2], servicio de detección y mitigación de amenazas en la red utilizando inteligencia artificial, cacería de amenazas continuas y análisis de brechas de seguridad de la superficie externa de la entidad y un equipo de respuesta a incidentes de seguridad (CSIRT) para la asistencia y remediación ante incidentes de ciberseguridad.

El servicio deberá ejecutar por un periodo de treinta y seis (36) meses garantizando la detección y respuesta efectiva de manera automatizada ante ataques cibernéticos sobre un total de al menos 140 SERVIDORES DE MISIÓN CRITICA (físicos, virtuales y nube) y 800 ESTACIONES DE TRABAJO, integrando las fuentes necesarias (antivirus, antispam, correo, firewalls, switches y componentes de red) para mejorar la tasa de detección y respuesta.

- El servicio deberá tener mínimamente el siguiente alcance técnico funcional:

Plataforma integral de orquestación, automatización y respuesta de ciberseguridad	• La plataforma tecnológica mínimamente requerida para ejecutar el servicio de detección y mitigación de ciberamenazas debe incluir el licenciamiento de hasta de 1000 (mil) activos, así como el mismo número de agentes (el uso de agentes será opcional, siempre y cuando la solución propuesta garantice el monitoreo activo y seguridad de los equipos remotos, que no se encuentran conectados a la red local o se conectan a través de VPN) de distribución para estos activos así mismo debe de integrar funcionalidades de:

[1] Equipo encargado de proteger la infraestructura de TI contra ataques cibernéticos. Su enfoque principal es la defensa proactiva y reactiva, utilizando herramientas y técnicas para identificar, contener y mitigar amenazas a la seguridad.
[2] Equipo encargado de realizar pruebas ofensivas de seguridad para identificar vulnerabilidades en los sistemas, aplicaciones, y redes de una organización. Su principal objetivo es simular ataques reales que podrían ser llevados a cabo por ciberdelincuentes, ayudando a fortalecer la postura defensiva del Blue Team

	○ El servicio deberá recolectar, procesar y analizar las consultas DNS (Domain **Name** Service) que los activos monitoreados realizan al Internet, a fin de detectar oportunamente la comunicación a infraestructuras ○ El servicio, deberá medir el compromiso de todos los activos de red monitoreados en tiempo real. ("Activo" todo elemento qué tenga asignada una IP y utilice infraestructura de comunicaciones para salir a navegar por internet) ○ El servicio deberá recolectar, procesar y analizar metadatos de red en dispositivos remotos con sistema operativo Windows 10 y superior y Mac de Apple y Linux. ○ El servicio, tendrá la capacidad de recolectar, procesar y analizar los Netflows, Logs de Proxy, Logs de Firewalls, Logs de los servidores y los correos electrónicos tipo SPAM a fin de identificar probables ataques a la infraestructura tecnológica por este medio. En caso sea necesario utilizar puertos SPAN/TAP el contratista deberá considerar la tecnología adecuada para recolectar los Syslogs necesarios (como parte de la solución propuesta, considere la necesidad de utilizar un hardware especializado para la recolección de syslog, deberá proporcionarlo como parte de la solución ofertada) ○ El servicio, deberá recolectar los datos de los dispositivos monitoreados y medir el compromiso, sin hacer uso de hardware de propósito específico, tales como Network TAPs (Terminal Access Point), entre otros: ▪ La medición del compromiso no debe estar basada en el análisis de archivos tipo PCAP (Packet Capture). ▪ La medición del compromiso deberá estar basado en el análisis de la metadata de los datos recolectados y clasificar el resultado de la medición del compromiso, por ejemplo: Malware, C&C (Command & Control), Phishing y mining. • El servicio, tiene qué mantener una retención histórica de los datos recolectados de hasta 02 años. Los datos recolectados pueden ser guardados en nube y/o en almacenamiento local (Hardware) de responsabilidad del contratista. (instalación, mantenimiento, gastos relacionados con su instalación como espacio de rack y cualquier otro gasto relacionado con su instalación y mantenimiento). ○ El contratista podrá mantener el histórico en una nube, privada (del contratista) y en caso de ser una pública, pagada y mantenida por el contratista, siempre y cuando cumpla con requerimientos de seguridad, según el NIST y/o el NTP-ISO/IEC 27001 y/o SOC 2 tipo 2. • El servicio, deberá contar con la capacidad de identificar, mitigar y remediar las amenazas detectadas, utilizando de manera efectiva la infraestructura de seguridad TI desplegada. • El servicio, deberá de actualizar las listas "negras" de las capas de ciberseguridad (Firewall y Endpoint) de manera automática y con una periodicidad máximo de 01 minuto, para lograr la mitigación y remediación automática. • El servicio deberá ser independiente de la capa de seguridad implementada por la entidad y tendrá la capacidad de recolectar metadatos de red sin importar la(s) marca(s) de la misma. • Los colectores o "Virtual Appliance" empleados para colectar la información deberán ser gratuitos. El sistema proveerá los dispositivos necesarios que colectar información de forma pasiva, de acuerdo con el diseño que se elaborará en conjunto con la ENTIDAD, estos colectores de metadata se recolecta directamente de los equipos de seguridad de la ENTIDAD, los colectores en forma de appliance virtual, serán instalados en la infraestructura de la entidad y deberá soportar los hipervisores Virtual Box, Hyper-V y VMWare.

	• El contratista será responsable de la determinación de la cantidad de colectores o Virtual Appliance necesarios y de su despliegue para recolectar la información que necesite para cumplir con el servicio. • La solución deberá entregar a la entidad un portal web de administración (exclusivo de LA ENTIDAD) que sea compatible con los navegadores siguientes: Chrome, Firefox, Internet Explorer, Edge, Safari; así mismo, que tenga la capacidad de: ○ Mostrar estadísticas de los indicadores de compromiso. ○ Configurar opciones de filtros de tiempo predefinidos y personalizados. ○ Mostrar de forma agrupada los activos monitoreados de manera personalizada. ○ Configurar etiquetas personalizadas para clasificar ataques. ○ Descargar los indicadores de compromiso desde el portal web de administración. ○ Mostrar la relación entre el compromiso detectado y la matriz publicada por ○ The MITRE ATT&CK™ Framework, describiendo tácticas y técnicas de ataque asociadas. ○ Mostrar información de los correos electrónicos tipo SPAM analizados, por ejemplo: ▪ Volumen de correos analizados, destinatarios con más correo malicioso o SPAM recibido. ▪ Tendencias de ataques el cual hace referencia a un análisis de tiempo para verificar y revelar patrones, como picos de SPAM en ciertas épocas del año. ▪ Configurar etiquetas personalizadas para clasificar ataques. • La plataforma deberá contar con Inteligencia Artificial que tengan algoritmos de aprendizaje automático que pueden analizar grandes volúmenes de datos para identificar patrones de ataques, lo que mejorará la detección de amenazas y reducirá los falsos positivos.
Capacidades de prevención y reducción de superficie de ataque	El servicio deberá de incluir el escaneo avanzado, monitoreo de la dark web[3] y tecnología de punta, utilizando técnicas para evaluar la postura de ciberseguridad externa de un dominio de la ENTIDAD y con capacidad de: • Mapear la superficie de ataque externa de la organización para identificar brechas de visibilidad externa y riesgos de seguridad. • Priorizar las actividades de remediación con base en el nivel de riesgo que representan para el negocio • Priorizar las actividades de remediación • Proteger a los usuarios con mayor riesgo, el cual deberá ser determinado por el postor • Neutralizar riesgos de infostealer. • Superar la ventaja de los atacantes. • Scanear las IP's públicas asociadas a (los) dominio(s). • Monitorear los Puertos abiertos. • Scanear las vulnerabilidades asociadas (que tengan expuesto un servicio web, o puerto de escritorio remoto a través de una ip pública, falta de parches, etc.). • Monitorear a los empleados comprometidos con malware del tipo Infostealer tales como: Redline, Recordbreaker, Xfilestealer, Lummastealer, Raccoon, entre otros, y la cantidad de credenciales exfiltradas, así como su tendencia en el tiempo. • Se deberá entregar un reporte semestral de TAKEDOWNs. • El número de TAKEDOWNs deberá ser ilimitado y automatizado. El servicio de SOC debe cubrir todo el ciclo de vida de una alerta, desde que se inicia hasta que se soluciona, permitiendo a la institución tener completo conocimiento de la gestión de cada incidente mediante la consola de

[3] Los reportes de la Dark Web deberán ser mensuales.

	administración del servicio, así como por medio de alertas mediante correo electrónico. El servicio debe detectar en tiempo real las conexiones de los sitios protegidos, entregando como mínimo la siguiente información: IP, Fechas, Horas, Información de Geolocalización, URL de conexión, URL de origen. El servicio deberá proveer detección de conexiones a través de proxies anónimos y/o cualquier otro canal de conexión que atente contra la integridad del sitio protegido. Es necesario que esta característica no implique instalar ningún ejecutable del lado usuario. El servicio deberá proveer detección de conexiones que provengan de fuentes sospechosas en tiempo real. El servicio debe tener la capacidad de analizar el origen de las conexiones, detectando y bloqueando las que vengan de países riesgosos en cuanto a actividad maliciosa. El servicio de monitoreo deberá detectar el registro de nuevos dominios en Internet, que guarden semejanza con el sitio protegido. El servicio deberá proveer la funcionalidad de informaciones forenses de evidencias de ataques documentadas en los tickets El servicio de monitoreo debe estar en la capacidad de detectar cualquier comportamiento anómalo de navegación y/o uso de los sitios web protegidos, tales como, copia del sitio protegido, redireccionamiento, etc. El servicio deberá estar en la capacidad de detectar y desactivar amenazas o ataques en contra las páginas web de la SUNASS, tales como malware, Man-in-the-Middle y Man-in-the-Browser. La solución debe tener la capacidad de monitorear y detectar aplicaciones móviles maliciosas. El servicio deberá estar en capacidad de monitorear todas las principales tiendas de aplicativos móviles y una amplia gama de tiendas de terceros o no oficiales, con el objetivo de detectar aplicaciones que intenten hacer uso indebido de la marca y/o el nombre de la institución. El servicio deberá estar en capacidad de brindar protección contra Aplicaciones Móviles No Autorizadas, que estén siendo atacadas para robar datos de clientes o para instalar malware, mediante el uso indebido de la marca y/o el nombre de la institución. Por lo tanto, se debe contar con un servicio de identificación y remoción de esas aplicaciones. El servicio brindado no deberá implicar la compra de hardware para el servicio y almacenamiento a la institución El contratista seleccionado debe tener la capacidad de realizar detección de registro de dominios similares al de la SUNASS y mostrar esta información a través de un portal web con la siguiente información como mínimo: ○ Fecha de alerta ○ Dominio Similar ○ Registro MX (indicar si tiene registro MX activo) El servicio deberá complementarse con componente humano encargado de monitorear la información obtenida de las redes sociales, dark web, entre otros para identificar la propagación de fraude (captación de credenciales) en estos medios y gestionar su desactivación. El servicio tendrá la capacidad de consumir y procesar los Weblogs de los portales monitoreados con el objetivo de realizar detección de incidentes de fraude. La solución debe contar con otros mecanismos que aumenten la proactividad del servicio, tales como JavaScript insertables en los portales web transaccionales monitoreados. El servicio deberá estar en la capacidad, cuando sea viable técnicamente, de identificar si los usuarios víctimas de sitios fraudulentos detectados ingresaron información y de ser posible obtener la información que ingresaron. Las "Capacidades de prevención y reducción de superficie de ataque", puede ser diferente siempre y cuando la visualización sea integrada y orquestada en la solución ofertada y no se requiera ir a cada herramienta para ver los resultados
Capacidades de detección de amenazas	La capacidad de detección y alerta temprana debe cubrir las 24 horas del día, los 07 días de la semana los 365 días del año detectando amenazas como consecuencia de rutinas de detección automáticas y personal calificado que

cibernéticas y actividad inusual de usuarios	notifique, explique y asista en el desarrollo de cualquier incidente, solicitando mínimamente que: • La plataforma deberá detectar la actividad de criptominería de los mineros de criptografía basados en navegadores, así como el software de cliente de criptominería común. • La plataforma deberá detectar inicios de sesión fuera de los países esperados o direcciones IP maliciosas conocidas. • La plataforma deberá informar sobre los datos de registro de Microsoft Office 365, Azure y Microsoft Exchange. • La plataforma deberá monitorear los cambios en las cuentas de usuario en Active Directory y sincronizará los cambios en la consola o plataforma. Opcionalmente el administrador podrá reportar cambios en la Consola. • El servicio deberá considerar la detección de eventos considerados como amenazas, que tengan un potencial de causar daño o impacto. Los eventos incluyen el acceso no autorizado a las computadoras, el uso no autorizado de los privilegios del sistema y la ejecución de malware que destruye, cifra un sistema o roba datos. Teniendo en cuenta que: - Un evento se considera como una ocurrencia observable, como cuando se produce un inicio de sesión fallido en una computadora. Si bien esto podría ser intencional o no intencional, ambos se consideran eventos. - Un incidente de seguridad es una violación o amenaza inminente de las políticas de seguridad o las mejores prácticas de la industria. • El servicio deberá poder detectar eventos relacionados mínimamente a: - Denegación de servicio - Phishing - Malware - Ransomware - Secuestro de RDP - PowerShell - PowerShell sin PowerShell - Compromiso de EMAIL (Business Email Compromise - BEC) - Ataque de intermediario (Man-in-the-middle attack - MITM) - Explotación de día cero - Cryptojacking (minería de criptomonedas maliciosa) - Túnel DNS - Ataque Drive-by - Ataque de espionaje • Los eventos que se necesitan registrar mínimamente para Sistemas Operativos Windows: 104 Se borró el registro de seguridad del sistema, 1102 Security - Se borró el registro de auditoría, 4722 - Security - Se habilitó una cuenta de usuario, 4735 - Security - Grupo local cambiado, 7040 - System - El servicio se cambió de inicio automático a deshabilitado, 7034 - System - Servicios terminados inesperadamente, 4702 - Security - Se modificó una tarea programada, 5142 - Security - Se agregó un objeto de recurso compartido de red, 5144 - Security - Se eliminó un objeto de recurso compartido de red, 4625 - Security - Una cuenta no pudo iniciar sesión, 7036 - System - Un servicio defensivo fue detenido, 5145 - Security - Se ha comprobado un objeto de recurso compartido de red por PsExec, 4649 - Security - Se detectó un ataque de repetición, 64004- System - Protección de archivos de Windows no pudo restaurar el archivo a su versión original, 5143 - Security - Se modificó un objeto de recurso compartido de red, 4740 - Security - Se bloqueó una cuenta de usuario, 4698 - Security - Se ha creado una nueva tarea programada, 7031 - System - El servicio finalizó inesperadamente,

	4738 - Security - Se ha cambiado la contraseña de la cuenta de usuario, 4724 - Security - Se ha intentado restablecer la contraseña de una cuenta, 4720 - Security - Cuenta de usuario de prueba creada y 1100 - System - Se cerró el registro de eventos. • Los eventos que se necesitan registrar mínimamente para sistemas operativos Mac: Log Privacy - Privatizar el contenido de registro que contiene nombres de usuario, direcciones IP y otra información confidencial. Watch_Logon - Inicios de sesión de usuario en el sistema, SSH_connection - Conexiones SSH entrantes a la Mac, Watch_Logout Cierres de sesión del usuario del Sistema, Failed_Auth - Error de autenticación de usuario, Sudo_Usage - Escalada de privilegios usando sudo. • Los eventos que se necesitan registrar mínimamente para sistemas operativo Linux: Sudo_Usage - Escalada de privilegios usando sudo, SSH_login - Conexiones SSH entrantes a la Mac, SSH_failed login - Error en los inicios de sesión SSH entrantes, User_add - Se ha creado una nueva cuenta de usuario, Password_change - Se ha cambiado la contraseña de un usuario, Group_change - Se cambió un grupo, Del_user_group - Se ha quitado un usuario de un grupo, Failed_Auth - Error de autenticación de usuario, SSH_login_pkey - Se detectó correctamente el inicio de sesión de clave pública a través de SSH, SSH_login_pkey_failed - Error al iniciar sesión con clave pública a través de SSH, user_del - Se ha eliminado una cuenta de usuario, new_group - Se creó un nuevo grupo, add_user_group - Se agregó un usuario a un grupo. El servicio debe poder gestionar de forma inteligente casos de phishing, poder identificar los usuarios que entran, cuantas veces ingresan a la solución, desde que dirección IP, su geolocalización, entre otros, mostrando la evidencia. El servicio debe tener un procedimiento progresivo que permita disminuir el riesgo del ataque de phishing hasta su desactivación final este procedimiento debe poder ser verificable por el cliente. El servicio debe tener la capacidad de recibir los correos electrónicos de los usuarios (abuse boxes), procesarlos para detectar posibles casos de fraude. El servicio deberá contar con funcionalidades de machine learning u otros mecanismos para analizar la probabilidad de que las URL´s sean phishing o malware. El contratista seleccionado debe hacer un acompañamiento periódico (por lo menos una vez al mes) puesta en producción el servicio, de manera de poder detectar posibles mejoras, requerimiento de crecimiento, entre otros. El servicio debe contar con una funcionalidad de monitoreo, protección y prevención contra amenazas en redes sociales (incluyendo monitoreo de perfiles VIP), mostrar menciones de la marca en dichas redes y permitir gestión para desactivación de esas amenazas ante dueños de redes sociales. El servicio debe monitorear las menciones en redes sociales como Twitter, Facebook y Google+, entre otros, dependiendo de la información que entregue cada una de estas redes sociales, de acuerdo con sus políticas de seguridad. El servicio deberá permitir la definición de palabras clave definidas por la institución para realizar las búsquedas relevantes de menciones en redes sociales. El servicio deberá disponer de una interfaz gráfica donde se registren las publicaciones realizadas en las redes sociales. El servicio deberá incluir la detección y desactivación de perfiles y/o cuentas falsas en redes sociales que suplanten la identidad de los funcionarios, de la institución, siempre y cuando dichos perfiles estén siendo usados para engañar a los usuarios o propagar fraude.

	El servicio ofertado deberá tener la capacidad de realizar detección y desactivación de incidentes que estén haciendo uso de la marca protegida. La desactivación de incidentes se debe realizar tanto en redes sociales como en páginas que de forma no autorizada y de manera ilegal estén haciendo uso de la marca protegida. La solución debe permitir monitorear ejecutivos y personal de alto valor dentro de la entidad mediante la inclusión de keywords. El servicio ofertado debe tener la capacidad de realizar desactivaciones de aplicaciones incluso si estas son una copia exacta de la original. En la información de cada incidente relacionado con aplicaciones se debe proporcionar información adicional como: o Nombre de la tienda o URL de descarga o Nombre del archivo (filename) o Versión de la aplicación o Sistema Operativo (Android o IOS) o Hash (MD5 y SHA256)" El servicio de monitoreo deberá notificar alertas a través de diversos canales de comunicación, tales como, correo electrónico, portal de administración, entre otros. El servicio debe estar contemplado mínimamente para: o Una (01) marca comercial "SUNASS " o Un (02) Dominios web que la entidad indique proteger o Redes Sociales en Facebook, Twitter, Instagram, LinkedIn, entre otras, asociadas a "SUNASS "
Capacidades de respuesta ante un evento de seguridad cibernética	• El servicio de respuesta debe darse como consecuencia de un análisis basado en: - La búsqueda de signos de comportamiento del adversario, indicadores de compromiso (IOC), hash de archivos de malware, URL, nombres de dominio y otros artefactos de compromiso anterior recopilando señales de cómo el adversario interactuó con plataformas y aplicaciones específicas para encontrar una cadena de comportamiento anómalo o sospechoso antes de dañar los sistemas. • Deberá colectar datos mediante escáneres activos, escáneres pasivos (análisis de tráfico de red) y agentes. No deberá haber límites en la cantidad de escáneres a desplegar en forma distribuida. • Deberá estar basado en un catálogo propio de vulnerabilidades que incluyan más de 160 mil evaluaciones diferentes y al menos 64 mil vulnerabilidades conocidas por un período no menor a 15 años. • Deberá proveer un mecanismo de priorización de vulnerabilidades automático basado en la probabilidad de explotación y que ofrezca información alternativa al CVSS (Common Vulnerability Scoring System) basada en Inteligencia de amenazas reales recabada de diversas fuentes como Deep Web, Dark Web, redes sociales, sitios de divulgación y otros centros de investigación. • Deberá ser capaz de evaluar, no solo vulnerabilidades, sino auditar configuraciones y compararlas contra las mejores prácticas y frameworks de seguridad tales como CIS, CERT, CISA STIG, PCI y otros para la totalidad de activos licenciados, incluidos equipos de red, infraestructura de virtualización, Windows, Linux, Bases de Datos, Aplicaciones y otros sistemas. Estas auditorías podrán ser personalizables por la organización. Se requiere esta capacidad sin límites de licenciamiento. • La solución deberá contar con una API completa para integración mediante scripting automatizado y exportación de datos mediante llamados. Esta API deberá estar liberada y documentada y no deberá tener limitaciones de licencias en cantidad de llamados o sistemas que la consultan. Si no existe una licencia ilimitada, considerar la de mayor capacidad disponible. • Los escáneres deberán ser desplegables en modalidad software y virtual appliance con soporte de VMware y Hyper-V.

	• Deberá permitir la configuración y almacenamiento seguro de credenciales de usuario para escanear mediante cuentas locales y de dominio Windows, cuentas ssh para sistemas Unix/Linux y dispositivos de red. Deberá permitir elevar privilegios mediante "su" y "sudo" y no deberá tener limitaciones en cantidad de credenciales. Además, el sistema deberá integrarse con soluciones de bóvedas digitales como Cyberark, Centrify, Beyondtrust y otras. • Deberá ser capaz de obtener vulnerabilidades de estaciones de trabajo en Internet (teletrabajo) y otros ambientes no conectados a la red del organismo, e inalcanzables por un escáner, mediante agente Windows, Linux y MacOS. • Deberá contar con escaneos que solo auditen la existencia o inexistencia de parches de todo tipo de sistemas (Windows Desktop, Unix/Linux, equipos de red, aplicaciones y otras plataformas). • Deberá mantener registro de estado de vulnerabilidades por activo, de modo de identificar vulnerabilidades que, habiendo sido remediadas, volvieron a surgir en nuevos escaneos. Deberán registrarse las fechas de primera aparición, última aparición y reaparición. Además, se deberá contar con una vista de vulnerabilidades remediadas. • Deberá ser capaz de identificar sistemas comprometidos por malware y otros códigos maliciosos. También deberá ser capaz de identificar la ejecución y nivel de firmas del sistema de Antimalware presente en el dispositivo. • Deberá reportar vulnerabilidades que sean explotables, establecer el nivel de madurez del código de exploit (si aplica), documentar de qué forma se explota (malware, acceso remoto, con o sin credenciales), si el exploit está presente en frameworks reconocidos tales como Metasploit, Canvas, Core y otras. • Deberá ser capaz de integrarse a un Centro de Operaciones de Seguridad (SOC) mediante alertas automatizadas independientes y nativas en el producto, así también integrarse a una solución de SIEM y de Orquestación (SOAR)[4]. Indicar la capacidad de integración con Splunk, IBM QRadar, LogRhythm, Siemplify, Simlane y otros. Se espera que la solución alerte cuando se detecten nuevas vulnerabilidades críticas en sistemas relevantes, nuevas vulnerabilidades asociadas a una amenaza conocida y otras reglas personalizables. • Deberá soportar la integración con sistemas de ticketing externos. • La solución debe proporcionar un modelo de licencia dinámico, para garantizar que la recopilación de datos (escaneos activos o detección pasiva) no se interrumpa cuando se rebase temporalmente las licencias contratadas. Además, la solución deberá contar con la posibilidad de informar el conteo de licencias utilizado y licenciado y las fechas de expiración.

8.2 NIVELES DEL SERVICIO

- El SERVICIO debe escalar un evento de interés a un incidente de forma automática o manual; los incidentes deben generar una notificación por EMAIL o un ticket de mesa de ayuda cuando la integración esté habilitada.
- El SERVICIO debe escalar aún más un incidente llamando al cliente o aislando el dispositivo y llamando al cliente. Cuando se detecta una ejecución potencialmente maliciosa en un dispositivo, el EQUIPO del contratista lo manejará como un incidente de Gravedad 1 hasta que la institución comunique lo contrario.
- Después de que el primer evento sospechoso/malicioso se convierta en un incidente, los analistas buscarán otros eventos e incidentes inusuales y que lo corroboren.
- Las aplicaciones sirven como recopiladores de eventos; el SERVICIO evaluará regularmente los eventos en las aplicaciones para buscar cualquier instancia que deba

[4] Es responsabilidad del postor incluir dentro de su propuesta de solución la herramienta de Orquestación, automatización y respuesta de seguridad (SOAR).

escalarse a un incidente o crear una regla lógica para generar notificaciones automáticamente.

- El tiempo de detección, los patrones de telemetría y la zona horaria del cliente son muy importantes para los analistas del SERVICIO y la acción que tomarán. El EQUIPO tiene en cuenta la zona horaria de la institución y las ejecuciones fuera del horario laboral en el proceso de toma de decisiones.
- El EQUIPO debe iniciar una investigación en profundidad luego de cualquier incidente/evento de Severidad 1 para determinar si el historial de incidentes y los eventos en las aplicaciones presentan algún otro indicio de un entorno violado. Según lo que encuentre, el SOC deberá aislar los dispositivos si:
  - La SUNASS no responde la llamada para confirmar que las acciones están autorizadas.
  - El EQUIPO que brinda el SERVICIO contratado no puede determinar con 100 % de certeza que alguna etapa de un ataque no está en curso en función de los incidentes y eventos encontrados en el panel del cliente en ese momento por lo que la rutina dispara aislamiento y confirmación por defecto.

NIVELES DE GRAVEDAD – EVENTOS / INCIDENTES				
SEVERIDAD	IMPACTO	DESCRIPCIÓN	RESPUESTA TÍPICA (DETECCIÓN/NOTIFICACIÓN/ACCIÓN)	SLA (ACUERDO DE NIVEL DE SERVICIO)
SEV1	CRÍTICA	El sistema fue violado, ataque en curso.	-1min / -1min, / -1min	Max 60 min.
SEV1	CRÍTICA	AV no pudo ponerse en cuarentena. Malicioso, sospechoso, ejecuciones o archivos inusuales. Entrada exitosa conexiones de direcciones IP de mala reputación o países monitoreados.	--1min / -1min, / -1min	Max 60 min.
SEV2	IMPORTANTE	Actividad inusual, pero sin incumplimiento por parte de malintencionados se detectó un evento y ningún sistema o los componentes estaban comprometidos.	-1min / -1min, / -1min	No aplica
SEV3	MENOR	El sistema muestra intentos de inicio de sesión fallidos u otros eventos generados por la red del cliente sistemas o usuarios y no forman parte de una amenaza de ciberseguridad.	2 min. / 10 min. / según sea necesario	No aplica
SEV4	INFORMATIVA	No se observa ningún efecto malicioso en el sistema.	2 min. / según sea necesario / según sea necesario	No aplica

8.2.1 Área de trabajo del contratista

El área de trabajo será en los Centro de Control del CyberSOC del Contratista o de la plataforma de SOC administrada que utilice para brindar el servicio, el cual debe de ser GEO redundante, mayor a 99 % en modalidad de alta disponibilidad.

8.2.2 Requerimientos técnicos

- Elaborar Los servicios y equipamiento descritos correrán por cuenta del CONTRATISTA.
- En caso de que la arquitectura de funcionamiento sea basada en agente, solo se demandará acceso a la consola principal del contratista para el tratamiento de los eventos por el puerto que se indique.

8.2.3 Controles de atención disponible

El CONTRATISTA debe poner a disposición los siguientes canales de atención y comunicación, al día siguiente de suscrito el contrato:

- Telefónico. - A través de medios de telefonía fija o móvil, se debe entregar una cartilla trimestral de atención de contacto.
- E-mail y Chat. - A través de comunicación electrónica como e-mail y chat (mensajería instantánea). Para el caso de e-mail, se recibirán consultas o solicitudes de soporte en la dirección de correo que se establezca.
- Atención Remota (control remoto). - Se ejecutará mediante procedimientos especiales de conexión remota, La conexión remota debe ser establecida mediante conexión VPN o conexión a escritorio remoto mediante software cliente certificado y seguro.

8.2.4 Elaboración de los Productos y Entregables.

El servicio deberá contar como mínimo con las siguientes etapas, las cuales deberán ser documentas y presentadas.

A) Plan del trabajo e implementación del servicio (P01)

A.1) Plan de trabajo

- El plan de trabajo debe contener las etapas de implementación del servicio de ejecución y metodología. Debe presentarse como plazo máximo 5 días calendarios siguientes a la fecha de la suscripción del contrato. Debe ser aprobada a los 2 días por el área de Infraestructura Tecnológica, en caso de haber subsanaciones se le dará un plazo máximo de 3 días calendarios.
- Como parte de la metodología debe presentar el documento Plan de Implementación del Servicio que debe contener como mínimo:

  - El alcance del proyecto.
  - El cronograma de implementación,
  - Los interesados,
  - Los riesgos asociados,
  - La metodología de trabajo y gestión de incidentes,
  - Definición de indicadores de rendimiento
  - El equipo de trabajo y
  - Los hitos del proyecto.
  - Definición de:
    - ✓ La gestión de altas, bajas y cambios de configuración en los dispositivos de seguridad
    - ✓ Monitoreo del desempeño de la infraestructura
    - ✓ El proceso de manejo de incidentes de seguridad

- ✓ Los Reportes sobre la operación del sistema
- ✓ Servicio de ciberinteligencia
- ✓ Indicadores de rendimiento
- ✓ Gestión de requerimientos
- ✓ Gestión de cambios
- ✓ Gestión de configuraciones
- ✓ Gestión de niveles de servicio
- ✓ Servicio de monitoreo
- ✓ Integración
- ✓ Respuesta a incidentes

- El cronograma del plan trabajo de la etapa de implementación debe incluir la siguiente información:
  - Nombre de la etapa.
  - Nombre de la actividad.
  - Plazos para cada actividad.
  - Duración de la actividad
  - Fecha de inicio de la actividad.
  - Fecha de fin de la actividad.
  - Responsable de la actividad.

- Para cada una de las etapas del servicio el CONTRATISTA debe identificar los riesgos que afecten cada una de sus etapas.

A.2) Implementación del servicio

- El plazo máximo para la implementación del servicio es de hasta 30 días calendarios, contados desde el día siguiente de suscrito el contrato, dentro del cual se suscribirá el acta de inicio del servicio.

En esta etapa debe realizarse todas las implementaciones necesarias relativas a:

- Despliegue de los agentes[5] de monitoreo, detección y respuesta a incidentes, sobre los servidores seleccionados para este servicio:
  - Asegurar la comunicación de estos con la plataforma de SOC (Cyber Security Operations Center).
  - Descubrir y documentar el acceso privilegiado a estos recursos.
  - Documentar el nivel de criticidad en función a la disponibilidad, integridad y privacidad de los activos.

- Se debe desplegar los agentes de monitoreo, detección y respuesta a incidentes, sobre estaciones de trabajo con acceso privilegiado a recursos de misión crítica en la institución

- Se debe reconocer y clasificar los sistemas, aplicaciones y software; necesarios para la ejecución de los servicios

- Se debe proceder con la configuración de los sistemas a instalar del Contratista y la vinculación con el equipamiento y sistemas que se requieran

- Se debe proceder con las búsquedas de credenciales comprometidas sobre diversas fuentes incluyendo dark web, Telegram y otros.

- Se debe programar las actividades de reducción de superficie de ataque con objetivos

[5] El uso de agentes será opcional, siempre que la solución propuesta garantice el monitoreo para el análisis y respuesta de incidentes de toda la red, de toda la infraestructura y de todos los usuarios de Sunass.

de reducción del riesgo mensual.

- Establecer los canales de comunicación entre el Contratista y La SUNASS para la mesa de ayuda y registro de ocurrencias.

- Presentación de Informe de la implementación del servicio

B) Operación del servicio

Esta etapa inicia luego de concluida la etapa de implementación en la cual se suscribirá el acta de inicio del servicio y consiste en la parte de ejecución del servicio de monitoreo tal como está descrito en el numeral 8 punto 8.1.
Esta etapa tiene una duración de 36 meses, contabilizados luego de culminar la etapa de implementación en la cual se suscribirá el acta de inicio del servicio.

La operación debe tener ciclos mensuales. Al final de cada ciclo se debe presentar **reporte de operaciones del servicio** de cada una de las actividades descritas en el en el numeral 8 punto 8.1, el contratista deberá elaborar el reporte el cual deberá ser aprobado por el Coordinador designado por la Oficina de tecnología de la información, indicando los hechos más significativos como los siguientes:
P02 hasta P37: Reporte de operaciones del servicio:

1. Cobertura del servicio Servicio - Monitoreo de salud de la plataforma.

2. Monitoreo Avanzado
   - Estadística de eventos recopilados por mes.
   - Detalle de eventos de seguridad que generen incidentes y/o alertas.
   - Detalle de respuestas ante eventos.

3. Inteligencia de Amenazas y Threat Hunting
   - Actividad de hacking sobre activos específicos de la SUNASS (15 activos públicos).

4. Al final de cada ciclo, de forma mensual, el contratista deberá tener una reunión con el Coordinador designado por la Oficina de tecnología de la información y el Oficial de Seguridad y Confianza Digital, brindando el reporte y las recomendaciones necesarias para reforzar la seguridad a nivel tecnológico y de protocolos.

Debe contener un apartado, de ser el caso, de los hechos resaltantes que han sucedido en dicho ciclo.
Además, debe tener el reporte de todas las actividades conforme los niveles de servicio (SLA) establecidos descritos en el descrito en el numeral 8 punto 8.1.
El CONTRATISTA debe registrar todos los incidentes de manera automática efectuando un ticket en el sistema de mesa de ayuda de SUNASS. La SUNASS debe reportar todos los incidentes o problemas sucedidos sobre el alcance del servicio a través de los canales establecidos en la etapa de implementación del servicio. El CONTRATISTA está en la obligación de comunicar el registro de tickets en un plazo máximo de 15 minutos de reportada la incidencia. La notificación a la mesa de ayuda debe estar operativa 24x7x365 para el registro de ocurrencias.

8.3 OTRAS OBLIGACIONES DEL CONTRATISTA

El contratista es responsable directo y absoluto de las actividades que realizará, debiendo responder por el servicio objeto de contratación.

El contratista adicionalmente a las obligaciones que le corresponden, conforme a los dispositivos legales vigentes, y que son inherentes al servicio contratado, éste se obliga y compromete a cumplir con lo siguiente:

- Presentar los entregables de acuerdo con el plazo previsto en los Términos de Referencia, ante la dependencia designada para obtener la conformidad.
- Garantizar la participación del personal clave del servicio, otros descritos en su propuesta técnica y en el plan de trabajo.
- Aplicar la reglamentación, directivas, normas técnicas y demás documentos que sean de cumplimiento obligatorio para los procesos operacionales de las unidades operativas de la Sunass, durante el desarrollo del Servicio, así como para sustentar adecuadamente la documentación técnica que formulará.
- SUNASS, en aplicación de su derecho de fiscalizar y supervisar el desarrollo del servicio materia del presente contrato, podrá convocar el contratista, en las oportunidades que crea necesario, para efectuar coordinaciones y revisiones del avance obtenido en el desarrollo del servicio; así como para que informe o asesore en asuntos concernientes al objeto del contrato.
- El contratista, es responsable del personal que contrate y las obligaciones y beneficios que implique, quedando claro que SUNASS no mantiene vínculo laboral ni contractual con el personal que ejecute el servicio.
- Deberá contar con un Centro de Operaciones de Seguridad (SOC) para brindar el soporte 24x7x365 incluidos domingos y feriados.

9 REQUISITOS DEL CONTRATISTA Y/O PERSONAL

9.1 DEL CONTRATISTA:

Deberá tener como mínimo dos personas responsables del SOC:

a) Jefe del proyecto (01)

- Profesional Titulado y Colegiado de las carreras de Ingenierías de, Computación o Informática o Sistemas o Redes, Comunicaciones y/o Telecomunicaciones o Ingeniería Empresarial y de Sistemas o ingeniería en ciberseguridad o ingeniería en Administración y Sistemas o ingeniería de Sistemas e Informática o ingeniería de Sistemas de Información o ingeniería de Computación y de Sistemas o ingeniería de telecomunicaciones y redes o ingeniería de redes y comunicaciones o ingeniería en Seguridad Informática.
- El jefe del proyecto deberá tener al menos 03 años como jefe de Proyectos o Gestor de Proyectos o Coordinador de Proyectos relacionados con el servicio de SOC.
- La colegiatura y habilitación será acreditada al inicio de la implementación del Servicio.

Contar con las siguientes certificaciones como mínimo:

- Certificación en ITIL Foundation
- Certificación del Project Management Professional (PMP)
- Certificación en ISO/IEC 27001:2013 Auditor líder o ISO/IEC 27001:2022 Auditor Líder

Estas certificaciones se presentarán a la suscripción del contrato.

Contar con un diplomado o curso, mínimo 90 horas lectivas:

- Especialización en Gerencia o Dirección de Proyectos, o
- Especialización avanzada en gerencia de proyectos y calidad.

Funciones:

- Auditar, planificar y diseñar mejoras, implementar controles de seguridad, capacitar y concientizar, monitorear y realizar una evaluación continua de los controles alineando las actividades al cumplimiento y mejoramiento de los niveles madurez del framework de la NIST, exponer el informe de cada entregable y brindar las recomendaciones necesarias si hubiera, al Coordinador designado por la OTI.

b) Auditor e Implementador de mejoras continuas (01)

- Profesional Titulado, Colegiado y habilitado de las carreras de, Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería de Telecomunicaciones, Computación o Informática o Sistemas o Redes y Comunicaciones o ingeniería Empresarial y de Sistemas o Ingeniería en ciberseguridad o ingeniería en Administración y Sistemas o ingeniería de Sistemas e Informática o ingeniería de Sistemas de Información o ingeniería de Computación y de Sistemas o ingeniería informática y de sistemas o ingeniería de telecomunicaciones y redes o ingeniería de redes y comunicaciones o ingeniería en seguridad informática.
- Con experiencia profesional mínima de dos (02) años como auditor y/o supervisor y/o implementador en seguridad de la información y/o ciberseguridad, la experiencia será considerada a partir de la obtención del bachiller, el mismo que será verificado en la página del SUNEDU.

Contar con las siguientes certificaciones como mínimo:

- Certificación en ITIL Foundation
- Lead Cyber security Professional Certificate.
- Service Desk Leader Professional Certificate

Estas certificaciones se presentarán a la suscripción del contrato

La colegiatura y habilitación será acreditada al inicio de la implementación del Servicio.

Funciones que realizar:

- Auditar, planificar y diseñar mejoras, implementar controles de seguridad, capacitar y concientizar, monitorear y realizar una evaluación continua de los controles alineando las actividades al cumplimiento y mejoramiento de los niveles madurez del framework de la NIST.

9.2 PROCEDIMIENTO PARA CAMBIO DE PERSONAL CLAVE

Para la prestación de la contratación correspondiente, el CONTRATISTA utilizará el personal calificado especificado en su oferta, no estando permitido cambios, salvo por razones de caso fortuito o fuerza mayor debidamente comprobadas, sustentando los motivos mediante un informe que refrende dicho cambio. En estos casos, el Contratista deberá proponer a la Entidad, por escrito, a través de mesa de partes para su aprobación por parte de la OTI, el que deberá reunir y acreditar calificaciones profesionales iguales o superiores al personal requerido.

10. RECURSOS PARA PROVEER POR EL CONTRATISTA

El contratista es responsable de asegurar todos los recursos necesarios de personal y equipos de informática para el desarrollo de todas las actividades planificadas para la elaboración y entrega de todos los documentos de entrega del numeral 14.2 Presentación

de Productos y Entregables, en los plazos establecidos.

11. DOCUMENTOS PARA PRESENTACIÓN DE OFERTAS[6]

Deberá entregar la siguiente documentación al momento de la presentación de la oferta:

- Presentar membresía activa en FIRST o certificado como SOC Type 2 o SOC Type 3, la membresía o certificado deberá corresponder al postor o fabricante de la solución ofertada.
- El proveedor deberá acreditar para admisión de la oferta ser representante o distribuidor autorizado de al menos una marca de la solución ofertada, adjuntando una carta del o los fabricantes haciendo referencia al proceso.

12. DOCUMENTOS PARA SUSCRIPCION DE CONTRATO[7]

- Certificaciones solicitadas del personal clave señaladas en el numeral 9.1 de los términos de referencia.

13. RECURSOS A SER PROVISTOS POR LA SUNASS

- En caso de realizar reuniones de forma presencial, el Coordinador designado por la Oficina de tecnología de la información deberá de gestionar los espacios adecuados o coordinar de forma virtual (usando tecnologías de videoconferencias u otros mecanismos previamente coordinados con SUNASS) o mixtas
- Gestionar y facilitar al contratista, el acceso a documentos e información que se requiera para la elaboración de los productos solicitados en el servicio.
- Facilitar el acceso a las instalaciones de SUNASS en caso de ser necesario para el cumplimiento de las actividades del servicio.
- Proporcionar el ambiente para reuniones, con el debido equipamiento, en caso sea necesario la realización de reuniones de coordinación o presentaciones de productos elaborados, en forma presencial.
- Acceso a internet limitado con las restricciones del caso.
- Acceso a las plataformas tecnológicas, software y hardware, debidamente supervisados

14. LUGAR Y PLAZO DE EJECUCIÓN

14.1 LUGAR DE EJECUCIÓN

El servicio se ejecutará en calle Bernardo Monteagudo 210 - 216, Magdalena del Mar, Sede CENTRAL y de manera semipresencial. Para lo cual la SUNASS brindará las facilidades para que el personal del contratista pueda ingresar a relevar información, realizar coordinaciones, sostener las reuniones que sean necesarias para la ejecución del "El Servicio de monitoreo, prevención, detección y respuesta ante ciberataques para servidores de misión crítica SOC AAS (Cyber Security Operations Center)".

Las reuniones se podrán realizar usando tecnologías de videoconferencias u otros mecanismos previamente coordinados con SUNASS.

[6] Cuando los documentos no figuren en idioma español, se presenta la respectiva traducción por traductor público juramentado o traductor colegiado certificado, en atención al articulo N° 59.1 del RLCE

[7] Cuando los documentos no figuren en idioma español, se presenta la respectiva traducción por traductor público juramentado o traductor colegiado certificado, en atención al artículo N° 59.1 del RLCE

14.2 PLAZO DE EJECUCIÓN

El plazo máximo para la implementación del **P01** es de hasta 30 días calendarios, contados desde el día siguiente de suscrito el contrato, dentro del cual se suscribirá el acta de inicio del servicio.

El plazo para la ejecución del servicio es de 36 meses contabilizados desde la fecha establecida en el acta de inicio del servicio.

15. SISTEMA DE CONTRATACIÓN:
Suma alzada.

16. ENTREGABLES DEL SERVICIO

16.1 PRESENTACIÓN DE LOS PRODUCTOS Y ENTREGABLES

El contratista, deberá entregar productos cada 30 días calendarios. Después de cada producto mensual de Reportes de Operación de servicio, el contratista deberá realizar reuniones las cuales podrán realizar forma presencial, virtual (usando tecnologías de videoconferencias u otros mecanismos previamente coordinados con SUNASS) o mixtas, para explicar el reporte y dar recomendaciones si fueran necesarias en las cuales deberán participar los profesionales responsables del equipo técnico del contratista, Oficina de Tecnologías de Información de la SUNASS.

16.2 PRESENTACIÓN DE PRODUCTOS Y ENTREGABLES

La presentación de productos y entregables podrá realizarse de las dos (02) siguientes formas:

Por Mesa de Partes Presencial:

La versión final de todos productos y entregables deberá ser presentada impresa en tres (03) ejemplares, debidamente organizados y anillados. Adjuntándose un DVD/USB con:

- Los archivos en formatos originales (MS Word, MS Excel, MS Project, MS Visio, etc.)

- La versión final de los productos, en formato PDF con firma digital de los responsables del equipo técnico del contratista.

Por Mesa de Partes Virtual:

En formato electrónico (formato original de cada documento o anexo) a través de la mesa de partes virtual de SUNASS

http://notificaciones.sunass.gob.pe:8080/mesadepartes/inicio-general.

El presente servicio establece la presentación de seis (06) entregables que se indican en el siguiente cuadro:

	Productos	Plazo y condiciones
Entregable 1	**P01:** Plan de trabajo e implementación del servicio • Plan de trabajo • Informe de la implementación del servicio. **P02:** Reportes de operación del servicio **P03:** Reportes de operación del servicio **P04:** Reportes de operación del servicio **P05:** Reportes de operación del servicio **P06:** Reportes de operación del servicio **P07:** Reportes de operación del servicio	Para el P01, hasta 30 días calendarios, contados desde el día siguiente de suscrito el contrato, dentro del cual se suscribirá el acta de inicio del servicio. El primer reporte (P02) será presentado a los 30 días calendarios, a partir del día siguiente de la aprobación de P01. Para los P03, P04; P05, P06, P07, debe presentar cada 30 días un reporte de operación de servicio, contados a partir del reporte anterior respectivamente. Cada P02 al P07 serán entregados según numeral 8.2.4 inciso c)
Entregable 2	**P08:** Reportes de operación del servicio **P09:** Reportes de operación del servicio **P10:** Reportes de operación del servicio **P11:** Reportes de operación del servicio **P12:** Reportes de operación del servicio **P13:** Reportes de operación del servicio	Para los P08, P09, P10; P11, P12, P13, debe presentar cada 30 días un reporte de operación de servicio, contados a partir del reporte anterior respectivamente. Cada P08 al P13 serán entregados según numeral 8.2.4 inciso c)
Entregable 3	**P14:** Reportes de operación del servicio **P15:** Reportes de operación del servicio **P16:** Reportes de operación del servicio **P17:** Reportes de operación del servicio **P18:** Reportes de operación del servicio **P19:** Reportes de operación del servicio	Para los (P14, P15, P16; P17, P18, P19) debe presentar cada 30 días un reporte de operación de servicio, contados a partir del reporte anterior respectivamente. Cada P14 al P19 serán entregados según numeral 8.2.4 inciso c)

	Productos	Plazo y condiciones
Entregable 4	**P20:** Reportes de operación del servicio **P21:** Reportes de operación del servicio **P22:** Reportes de operación del servicio **P23:** Reportes de operación del servicio **P24:** Reportes de operación del servicio **P25:** Reportes de operación del servicio	Para los (P20, P21, P22;P23,P24,P25) debe presentar cada 30 días un reporte de operación de servicio, contados a partir del reporte anterior respectivamente. Cada P20 al P25 serán entregados según numeral 8.2.4 inciso c)
Entregable 5	**P26:** Reportes de operación del servicio **P27:** Reportes de operación del servicio **P28:** Reportes de operación del servicio **P29:** Reportes de operación del servicio **P30:** Reportes de operación del servicio **P31:** Reportes de operación del servicio	Para los (P26, P27, P28;P29,P30,P31), debe presentar cada 30 días un reporte de operación de servicio, contados a partir del reporte anterior respectivamente Cada P26 al P31 serán entregados según numeral 8.2.4 inciso c)
Entregable 6	**P32:** Reportes de operación del servicio **P33:** Reportes de operación del servicio **P34:** Reportes de operación del servicio **P35:** Reportes de operación del servicio **P36:** Reportes de operación del servicio **P37:** Reportes de operación del servicio	Para los (P32, P33, P34;P35,P36,P37), debe presentar cada 30 días un reporte de operación de servicio, contados a partir del reporte anterior respectivamente Cada P32 al P37 serán entregados según numeral 8.2.4 inciso c)

17. SUPERVISIÓN Y CONFORMIDAD

a. El control y seguimiento de las actividades que se desarrollarán en el marco del servicio

contratado, estará a cargo de un Coordinador designado por el jefe de la Oficina de Tecnologías de Información de la SUNASS.

b. SUNASS luego de la evaluación respectiva, podrá otorgar la conformidad a los productos y entregables, en caso contrario comunicará al contratista, las observaciones que considere, otorgándole un plazo para subsanar de acuerdo a la normativa vigente sobre contrataciones.

c. La conformidad de los entregables, será emitida por el jefe de la Oficina de Tecnologías, de información de la SUNASS, a través de un informe técnico previo, emitido por el coordinadordesignado por la Oficina de Tecnologías de Información y firmas de las Actas respectivas.

d. La conformidad será otorgada de acuerdo al Artículo 168 del reglamento de la ley de contrataciones del estado, por el Jefe de la Oficina de Tecnologías de Información, luego de verificado el cumplimiento de las condiciones contractuales.

18. FORMA DE PAGO

El pago se realizará de acuerdo con lo señalado en el Artículo 171 del Reglamento de la Ley de Contrataciones del Estado, luego de emitida la conformidad por el responsable de la Oficina de Tecnologías de Información, siempre que se verifiquen las condiciones establecidas en los términos de referencia. El pago se realizará en soles y en seis (06) armadas parciales, de acuerdo con el siguiente detalle:

Pago N°	% del monto total	Condición para el pago
Primer pago	20%	Conformidad del Entregable 1
Segundo pago	16%	Conformidad del Entregable 2
Tercer pago	16%	Conformidad del Entregable 3
Cuarto pago	16%	Conformidad del Entregable 4
Quinto pago	16%	Conformidad del Entregable 5
Sexto pago	16%	Conformidad del Entregable 6

Para proceder con el pago, el contratista deberá presentar sus entregables de acuerdo a lo descrito en el numeral 16.2 Presentación de Productos y Entregables, y la siguiente documentación:

- Documentación y/o contenido de cada producto según numeral ***8.2.4 Elaboración de los Productos y Entregables***
- Comprobante de pago
- Informe técnico del Coordinador designado por la Oficina de Tecnologías de Información de la SUNASS.
- Acta de conformidad del jefe de la Oficina de tecnologías de la Información-OTI.

19. PENALIDADES 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 SUNASS le aplica automáticamente una penalidad por mora por cada día de atraso, de conformidad con el Artículo 162 del Reglamento de la Ley de Contrataciones del Estado.

20. OTRAS PENALIDADES

De acuerdo con lo señalado en el Artículo 163 del Reglamento de la Ley de Contrataciones del Estado, se establecen las siguientes penalidades:

<table>
<tr><th colspan="5">Otras penalidades</th></tr>
<tr><th>N°</th><th>Supuestos de aplicación</th><th>Forma de cálculo</th><th>Aplicación</th><th>Procedimiento</th></tr>
<tr><td>1</td><td>En caso el contratista incumpla con su obligación de ejecutar la presentación con el personal acreditado o debidamente sustituido.</td><td>Media (0.5) UIT</td><td>Por cada día de ausencia del personal autorizado</td><td rowspan="4">La Oficina de Tecnologías de Información como área usuaria, emitirá un informe de conformidad de servicio a la Unidad de Abastecimiento donde se señale y sustente la falta incurrida (según corresponda).

Para la aplicación de una penalidad, la Sunass informará por escrito al CONTRATISTA, el mismo que tendrá un periodo de dos (02) días hábiles para efectuar su descargo. Si el descargo presentado por el CONTRATISTA no es aceptado por la Sunass, se procederá a ejecutar la penalidad correspondiente.</td></tr>
<tr><td rowspan="3">2</td><td rowspan="3">Por incumplimiento dentro del tiempo establecido en el acuerdo de nivel de servicio (SLA) como se menciona en el numeral 8.1 en la tabla NIVELES DE GRAVEDAD – EVENTOS/INCIDENTES</td><td>Una (01) UIT, por la primera vez que se presente</td><td rowspan="3">Por incidencia - Acuerdos de Niveles de Servicio (SLA)**</td></tr>
<tr><td>Dos (02) UIT, por la segunda vez que se presente</td></tr>
<tr><td>Dos y media (2.5) UIT, A partir de la tercera vez en adelante que se presente</td></tr>
<tr><td>3</td><td>Por utilizar y/o difundir, de manera indebida y sin autorización, a terceros la información relativa al servicio.</td><td>Dos (02) UIT, por cada incidencia que se detecte</td><td>Por incidencia - cumplimiento de Normativas de Sunass</td></tr>
<tr><td colspan="5">Advertencia
No se puede incluir como otras penalidades la sola presentación de la solicitud de autorización de sustitución del personal propuesto. La penalidad por sustitución del personal aplica siempre y cuando la SUNASS no haya autorizado su sustitución por no cumplir con la experiencia y calificaciones requeridas.</td></tr>
</table>

La Oficina de Tecnologías de Información (OTI), como área usuaria, emitirá un informe de conformidad del servicio, donde se señale otras penalidades aplicables según corresponda.
Importante:
La penalidad será descontada de la facturación correspondiente.
(*) Nota: Para la aplicación de las otras penalidades, se tomará en cuenta la UIT vigente según el año fiscal en que se ejecute el servicio.
(**) No se penalizará en caso la demora se deba a un problema en un equipo de infraestructura de la OTI que haya tenido que ser escalado con el fabricante del equipo, tampoco se penalizara en caso la demora se deba en un ticket generado por el postor hacia el fabricante de la solución del SOC

21. OTRAS CONSIDERACIONES DEL SERVICIO

21.1. SUBCONTRATACIÓN

No se permite subcontratación.

21.2. CONFIDENCIALIDAD

El contratista deberá mantener estricta confidencialidad sobre la información a la que tendrá acceso durante la ejecución del servicio. Asimismo, no podrá disponer de ésta para fines distintos al servicio que presta.

El contratista deberá de tener conocimiento de las "Disposiciones de seguridad de la información para proveedores" que serán comunicadas por la SUNASS si por la contratación el proveedor tiene acceso a algún activo de información de la SUNASS (sistemas de información, instalaciones de procesamiento, entre otros).

El contratista deberá de enviar al correo electrónico del personal responsable de la contratación del servicio la declaración jurada de compromiso de confidencialidad de proveedores de la Sunass firmada.

El proveedor podrá ser evaluado de acuerdo con los lineamientos de seguridad de la información. Dicha obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades y la información producida una vez que se haya concluido el servicio. Dicha información puede consistir en informes, documentos y demás datos recibidos, compilados o producidos por el proveedor.

21.3. OBLIGACIÓN ANTICORRUPCIÓN

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

Asimismo, el/la proveedor/a se obliga a conducirse en todo momento, durante la ejecución de la orden de servicio o 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/as, accionistas, participacionistas, integrantes de los órganos de administración, apoderados/as, representantes legales, funcionarios/as, asesores/as y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado. Además, el/la proveedor/a se compromete 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.

El incumplimiento de las obligaciones establecidas en esta cláusula faculta a SUNASS a resolver automáticamente y de pleno derecho la orden de servicio o el contrato, bastando para tal efecto remitir a EL CONTRATISTA una comunicación informando que se ha producido dicha resolución, sin perjuicio de las acciones civiles, penales y administrativas a que hubiera lugar.

21.4. CLÁUSULA ANTISOBORNO

21.4.1. El contratista declara conocer los compromisos antisoborno de la SUNASS, el cual se estable en su Política antisoborno y se encuentra disponible en el portal web de la SUNASS

21.4.2. (https://www.gob.pe/56299-superintendencia-nacional-de-servicios-de-saneamiento-sistema-de-gestion-antisoborno)

21.4.3. El contratista declara no haber, directa o indirectamente, ofrecido, negociado

o efectuado pago o, en general, entregado beneficio o incentivo ilegal en relación al servicio a prestarse o bien a proporcionarse. En línea con ello, se compromete a actuar en todo momento con integridad, a abstenerse de ofrecer, dar o prometer, regalo u objeto alguno a cambio de cualquier beneficio, percibido de manera directa o indirecta; a cualquier miembro del Consejo Directivo, funcionarios públicos, empleados de confianza, servidores públicos; así como a terceros que tengan participación directa o indirecta en la determinación de las características técnicas y/o valor referencial o valor estimado, elaboración de documentos del procedimiento de selección, calificación y evaluación de oferta, y la conformidad de los contratos derivados de dicho procedimiento.

21.4.4. El contratista se compromete a denunciar, sobre la base de una creencia razonable o de buena fe, cualquier intento de soborno, supuesto o real, que tuviera conocimiento a través del canal de denuncias de soborno ubicado en el portal web de la Sunass http://servicio.sunass.gob.pe/denuncias/.

21.5. PROPIEDAD INTELECTUAL

SUNASS adquirirá todos los derechos de propiedad intelectual necesarios para el aprovechamiento de los documentos y otros materiales que guarden una relación directa con la ejecución del servicio o que se hubiere creado o producido como consecuencia o en el curso de la ejecución del servicio.
En caso de que las prestaciones derivadas del contrato incluyan la creación de elementos considerados creaciones intelectuales, SUNASS adquirirá a título excluyente y por máximo plazo permitido por Ley, todos los derechos patrimoniales que la Ley otorgue sobre dicha creación a partir de la conformidad de la prestación.

21.6. INCIDENCIAS

El contratista deberá tener un respaldo del aplicativo del SOC durante la vigencia del servicio en caso de caída del mismo, para seguir las actividades el respaldo deberá ser implementado máximo en un periodo de 02 horas de la caída del servicio.

22. RESPONSABILIDAD POR VICIOS OCULTOS

La conformidad otorgada por SUNASS a la prestación del servicio no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos.

El plazo máximo de responsabilidad del contratista será de tres (03) años contado a partir de la conformidad de la SUNASS.

23. REQUISITOS DE CALIFICACIÓN

B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.3	**CALIFICACIONES DEL PERSONAL CLAVE**
B.3.1	**FORMACIÓN ACADÉMICA**
	01 Jefe de Proyecto Requisitos: • Profesional Titulado de las carreras de Ingenierías de, Computación o Informática o Sistemas o Redes, Comunicaciones y/o Telecomunicaciones o Ingeniería Empresarial y

	de Sistemas o ingeniería en ciberseguridad o ingeniería en Administración y Sistemas o ingeniería de Sistemas e Informática o ingeniería de Sistemas de Información o ingeniería de Computación y de Sistemas o ingeniería de telecomunicaciones y redes o ingeniería de redes y comunicaciones o ingeniería en Seguridad Informática. **Auditor e implementador de mejoras continuas** Requisitos: Profesional Titulado de las carreras de, Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería de Telecomunicaciones, Computación o Informática o Sistemas o Redes y Comunicaciones o ingeniería Empresarial y de Sistemas o Ingeniería en ciberseguridad o ingeniería en Administración y Sistemas o ingeniería de Sistemas e Informática o ingeniería de Sistemas de Información o ingeniería de Computación y de Sistemas o ingeniería informática y de sistemas o ingeniería de telecomunicaciones y redes o ingeniería de redes y comunicaciones o ingeniería en seguridad informática. Acreditación: El o Título Profesional requerido será verificado por el órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe// o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/, según corresponda. En caso el título profesional 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**
	01 Jefe de Proyecto Contar con un mínimo de 90 horas lectivas en diplomado o curso en: • Especialización en Gerencia o Dirección de Proyectos, o • Especialización avanzada en gerencia de proyectos y calidad. Acreditación: Se acreditará con copia simple de constancia o certificados de estudios u otros documentos según corresponda emitido por una entidad pública o institución privada. 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**
	01 Jefe de proyecto Requisitos: • El jefe del proyecto deberá tener al menos 03 años como jefe de Proyectos o Gestor de Proyectos o Coordinador de Proyectos relacionados con el servicio de SOC. 01 Auditor e implementador de mejoras continuas

Requisitos:

- La experiencia profesional mínima de dos (02) años como auditor y/o supervisor y/o implementador en seguridad de la información y/o ciberseguridad

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

Acreditación:

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

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.
- Cuando los documentos no figuren en idioma español, se presenta la respectiva traducción por traductor público juramentado o traductor colegiado certificado, en atención al artículo N° 59.1 del RLCE.

C.	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**

	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a ***Cuatro Millones con 00/100 Soles (S/ 4,000,000.00)***, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (08)) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se señala servicios similares a los siguientes: • ~~Servicios Servicio de Licencias de soluciones de seguridad o~~ Servicio de CYBERSOC o Administración y Monitoreo de Plataformas de Seguridad y Correlación Inteligente de Eventos de Seguridad • Servicio de monitoreo de eventos de seguridad (SOC) • Servicio de CyberSOC • Servicios de administración, operación, ~~soporte funcional y mantenimiento de Aplicaciones~~ monitoreo y respuesta ante incidentes (diseño e integración de nuevas fuentes, monitoreo y correlación de eventos, gestión respuesta a incidentes de seguridad, operaciones ofensivas, inteligencia de amenazas y análisis de riesgos de ciberseguridad) • Servicios de Centro de Operaciones de Seguridad (SOC) • Servicio de Inteligencia de Amenazas en la Red • Servicio de soporte a través de SOC (Security Opera Center), monitoreo y correlación de eventos para infraestructura de red y seguridad. • Servicio de ciberseguridad. 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 yfehacientemente, 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[8], 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, las veinte (20) primeras contrataciones indicadas en el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad. En el caso de servicios de ejecución periódica, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (08) 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 selecciónconvocados antes del 20.09.2012, la calificación se ceñirá al método descrito en laDirectiva "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 ala matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 09**.
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 servicio o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 8** referidoa la Experiencia del Postor en la Especialidad.

Importante

- *El comité de selección debe valorar de manera integral los documentos presentados por el postor para acreditar la 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, la calificación de la experiencia se realiza conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*
- *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 a.5) 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.*

3.2. REQUISITOS DE CALIFICACIÓN

B	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.3	**CALIFICACIONES DEL PERSONAL CLAVE**
B.3.1	**FORMACIÓN ACADÉMICA**
	01 Jefe de Proyecto Requisitos: • Profesional Titulado de las carreras de Ingenierías de, Computación o Informática o Sistemas o Redes, Comunicaciones y/o Telecomunicaciones o Ingeniería Empresarial y de Sistemas o ingeniería en ciberseguridad o ingeniería en Administración y Sistemas o ingeniería de Sistemas e Informática o ingeniería de Sistemas de Información o ingeniería de Computación y de Sistemas o ingeniería de telecomunicaciones y redes o ingeniería de redes y comunicaciones o ingeniería en Seguridad Informática[11]. **Auditor e implementador de mejoras continuas** Requisitos: • Profesional Titulado de las carreras de, Ingeniería Electrónica o Ingeniería de Sistemas o Ingeniería de Telecomunicaciones, Computación o Informática o Sistemas o Redes y Comunicaciones o ingeniería Empresarial y de Sistemas o Ingeniería en ciberseguridad o ingeniería en Administración y Sistemas o ingeniería de Sistemas e Informática o ingeniería de Sistemas de Información o ingeniería de Computación y de Sistemas o ingeniería informática y de sistemas o ingeniería de telecomunicaciones y redes o ingeniería de redes y comunicaciones o ingeniería en seguridad informática[12]. Acreditación: El Título Profesional requerido será verificado por el Órgano encargado de las contrataciones o comité de selección, según corresponda, en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: https://enlinea.sunedu.gob.pe// o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente link : *https://titulosinstitutos.minedu.gob.pe/* según corresponda. En caso el título profesional 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**
	01 Jefe de Proyecto Contar con un mínimo de 90 horas lectivas en diplomado o curso en: • Especialización en Gerencia o Dirección de Proyectos, o • Especialización avanzada en gerencia de proyectos y calidad.[13] Acreditación: Se acreditará con copia simple de constancia o certificados de estudios u otros documentos según corresponda emitido por una entidad pública o institución privada. **Importante**

[11] En atención a la absolución de la observación 7, efectuado por la empresa SONDA DEL PERU S.A.
[12] En atención a la absolución de la observación 8, efectuado por la empresa SONDA DEL PERU S.A.
[13] En atención a la absolución de la absolución de la consulta 40, de la empresa IMPERIA SOLUCIONES TECNOLOGICAS S.A.C. y consulta 71, 72 de la empresa ALLSAFE CORP E.I.R.L.

	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**
	01 Jefe de Proyecto Requisitos: • El jefe del proyecto deberá tener al menos 03 años como jefe de Proyectos o Gestor de Proyectos o Coordinador de Proyectos relacionados con el servicio de SOC. **01 Auditor e implementador de mejoras continuas** Requisitos: • La experiencia profesional mínima de dos (02) años como auditor y/o supervisor y/o implementador en seguridad de la información y/o ciberseguridad De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado. Acreditación: La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto. **Importante** • *Los 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.* Cuando los documentos no figuren en idioma español, se presenta la respectiva traducción por traductor público juramentado o traductor colegiado certificado, en atención al articulo N° 59.1 del RLCE.

C	**EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**

	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a **Cuatro Millones con 00/100 Soles (S/ 4,000,000.00)** por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se consideran servicios similares a los siguientes: • ~~Servicios Servicio de Licencias de soluciones de seguridad o~~[14] Servicio de CYBERSOC o Administración y Monitoreo de Plataformas de Seguridad y Correlación Inteligente de Eventos de Seguridad. • Servicio de monitoreo de eventos de seguridad (SOC) • Servicio de CyberSOC • Servicios de administración, operación, ~~soporte funcional y mantenimiento de Aplicaciones~~ monitoreo y respuesta ante incidentes[15] (diseño e integración de nuevas fuentes, monitoreo y correlación de eventos, gestión respuesta a incidentes de seguridad, operaciones ofensivas, inteligencia de amenazas y análisis de riesgos de ciberseguridad) • Servicios de Centro de Operaciones de Seguridad (SOC) • Servicio de Inteligencia de Amenazas en la Red • Servicio de soporte a través de SOC (Security Opera Center), monitoreo y correlación de eventos para infraestructura de red y seguridad. • Servicio de ciberseguridad.[16] 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[17], correspondientes a un máximo de veinte (20) contrataciones. En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad. En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados. En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato. Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de

[14] En atención a la absolución de la observación 2 y 17, de la empresa CYBER SECURITY ENTERPRISE S.A.C. y SONDA DEL PERU S.A, respectivamente.

[15] En atención a la absolución de la observación 18, 19 y 20, de la empresa SONDA DEL PERU S.A.

[16] En atención de la absolución de la observación, 44 de la empresa IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.g

[17] 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".*

	consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales. Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 9.** Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicios o de cancelación del comprobante de pago, según corresponda. Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 8** referido a la Experiencia del Postor en la Especialidad. **Importante** • *Al calificar la experiencia del postor, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del objeto contractual no coincida literalmente con el previsto en las bases, se deberá validar la experiencia si las actividades que ejecutó el postor corresponden a la experiencia requerida.* • *En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que se hayan comprometido, según la promesa de consorcio, a ejecutar el objeto materia de la convocatoria, conforme a la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado".*

Importante

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

CAPÍTULO IV
FACTORES DE EVALUACIÓN

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

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

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

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 MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE CIBERATAQUES PARA SERVIDORES DE MISIÓN CRÍTICA SOC AAS (CYBER SECURITY OPERATIONS CENTER)"**, que celebra de una parte [CONSIGNAR EL NOMBRE DE LA ENTIDAD], en adelante LA ENTIDAD, con RUC Nº [……], con domicilio legal en [……], representada por [……..…], identificado con DNI Nº [……], y de otra parte […….....], con RUC Nº [.....], con domicilio legal en […….....], inscrita en la Ficha N° […….....] Asiento N° […….....] del Registro de Personas Jurídicas de la ciudad de [……], debidamente representado por su Representante Legal, […….....], con DNI N° [……..], según poder inscrito en la Ficha N° [……..], Asiento N° [……] del Registro de Personas Jurídicas de la ciudad de [……], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

Con fecha [……..], el comité de selección adjudicó la buena pro del **CONCURSO PÚBLICO Nº003-2024-SUNASS** para la contratación del "SERVICIO DE MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE CIBERATAQUES PARA SERVIDORES DE MISIÓN CRÍTICA SOC AAS (CYBER SECURITY OPERATIONS CENTER)" a [INDICAR NOMBRE DEL GANADOR DE LA BUENA PRO], cuyos detalles e importe constan en los documentos integrantes del presente contrato.

CLÁUSULA SEGUNDA: OBJETO

El presente contrato tiene por objeto la contratación del "SERVICIO DE MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE CIBERATAQUES PARA SERVIDORES DE MISIÓN CRÍTICA SOC AAS (CYBER SECURITY OPERATIONS CENTER)".

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[18]

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.

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

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

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

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de [……..], 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].

CLÁUSULA SEXTA: PARTES INTEGRANTES DEL CONTRATO

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

CLÁUSULA SÉTIMA: GARANTÍAS

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

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

Importante

Al amparo de lo dispuesto en el numeral 149.4 del artículo 149 del Reglamento de la Ley de Contrataciones del Estado, en el caso de contratos periódicos de prestación de servicios en general, si el postor ganador de la buena pro solicita la retención del diez por ciento (10%) del monto del contrato original como garantía de fiel cumplimiento de contrato, debe consignarse lo siguiente:

"De fiel cumplimiento del contrato: [CONSIGNAR EL MONTO]*, a través de la retención que debe efectuar LA ENTIDAD, durante la primera mitad del número total de pagos a realizarse, de forma prorrateada, con cargo a ser devuelto a la finalización del mismo."*

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

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

CLÁUSULA NOVENA: 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 DÉCIMA: DECLARACIÓN JURADA DEL CONTRATISTA

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

CLÁUSULA UNDÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

La 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 tres (03) años contado a partir de la conformidad otorgada por LA ENTIDAD.

CLÁUSULA DUODÉCIMA: PENALIDADES

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

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

Donde:

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

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

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

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

OTRAS PENALIDADES

Otras penalidades				
N°	*Supuestos de aplicación*	*Forma de cálculo*	*Aplicación*	*Procedimiento*
1	*En caso el contratista incumpla con su obligación de ejecutar la presentación con el personal acreditado o debidamente sustituido.*	*Media (0.5) UIT*	*Por cada día de ausencia del personal autorizado*	La Oficina de Tecnologías de Información como área usuaria, emitirá un informe de conformidad de servicio a la Unidad de Abastecimiento donde se señale y sustente la falta incurrida (según corresponda). Para la aplicación de una penalidad, la Sunass informará por escrito al CONTRATISTA, el mismo que tendrá un periodo de dos (02) días hábiles para efectuar su descargo. Si el descargo presentado por el CONTRATISTA no es aceptado por la Sunass, se procederá a ejecutar la penalidad correspondiente.
2	Por incumplimiento dentro del tiempo establecido en el acuerdo de nivel de servicio (SLA) como se menciona en el numeral 8.1 en la tabla NIVELES DE GRAVEDAD – EVENTOS/INCIDENTES	Una (01) UIT, por la primera vez que se presente Dos (02) UIT, por la segunda vez que se presente Dos y media (2.5) UIT, A partir de la tercera vez en adelante que se presente	Por incidencia - Acuerdos de Niveles de Servicio (SLA)**	
3	Por utilizar y/o difundir, de manera indebida y sin autorización, a terceros la información relativa al servicio.	Dos (02) UIT, por cada incidencia que se detecte	Por incidencia - cumplimiento de Normativas de Sunass	
Advertencia *No se puede incluir como otras penalidades la sola presentación de la solicitud de autorización de sustitución del personal propuesto. La penalidad por sustitución del personal aplica siempre y cuando la SUNASS no haya autorizado su sustitución por no cumplir con la experiencia y calificaciones requeridas.*				

La Oficina de Tecnologías de Información (OTI), como área usuaria, emitirá un informe de conformidad del servicio, donde se señale otras penalidades aplicables según corresponda.
Importante:
La penalidad será descontada de la facturación correspondiente.
(*) Nota: Para la aplicación de las otras penalidades, se tomará en cuenta la UIT vigente según el año fiscal en que se ejecute el servicio.
(**) No se penalizará en caso la demora se deba a un problema en un equipo de infraestructura de la OTI que haya tenido que ser escalado con el fabricante del equipo, tampoco se penalizara en caso la demora se deba en un ticket generado por el postor hacia el fabricante de la solución del SOC

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

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

CLÁUSULA DÉCIMA TERCERA: RESOLUCIÓN DEL CONTRATO

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

CLÁUSULA DÉCIMA CUARTA: RESPONSABILIDAD DE LAS PARTES

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

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

CLÁUSULA DÉCIMA QUINTA: ANTICORRUPCIÓN

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

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

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

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

CLÁUSULA DÉCIMA SEXTA: MARCO LEGAL DEL CONTRATO

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

CLÁUSULA DÉCIMA SÉTIMA: SOLUCIÓN DE CONTROVERSIAS[19]

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.

El arbitraje será institucional, resuelto por ÁRBITRO ÚNICO y bajo la organización y administración del Centro de Análisis y Resolución de Conflictos de la Pontificia Universidad Católica del Perú.

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

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

CLÁUSULA DÉCIMA OCTAVA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

Cualquiera de las partes puede elevar el presente contrato a Escritura Pública corriendo con

[19] 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).

todos los gastos que demande esta formalidad.

CLÁUSULA DÉCIMA NOVENA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

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

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

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

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

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

"LA ENTIDAD"	"EL CONTRATISTA"

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley Nº 27269, Ley de Firmas y Certificados Digitales[20].

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

ANEXOS

“No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas”

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº003-2024-SUNASS

Presente.-

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

Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[21]		Sí		No	
Correo electrónico :					

Autorización de notificación por correo electrónico:

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.
2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios[22]

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.

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

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

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

ANEXO Nº 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº003-2024-SUNASS

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[23]		Sí		No	
Correo electrónico :					

Datos del consorciado 2					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[24]		Sí		No	
Correo electrónico :					

Datos del consorciado …					
Nombre, Denominación o Razón Social :					
Domicilio Legal :					
RUC :	Teléfono(s) :				
MYPE[25]		Sí		No	
Correo electrónico :					

Autorización de notificación por correo electrónico:

Correo electrónico del consorcio:

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

1. Solicitud de la descripción a detalle de todos los elementos constitutivos de la oferta.

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

[24] Ibídem.

[25] Ibídem.

2. Solicitud de reducción de la oferta económica.
3. Solicitud de subsanación de los requisitos para perfeccionar el contrato.
4. Solicitud para presentar los documentos para perfeccionar el contrato, según orden de prelación, de conformidad con lo previsto en el artículo 141 del Reglamento.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicios[26]

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.

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

ANEXO Nº 2

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº003-2024-SUNASS

Presente.-

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

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

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

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

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

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

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

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

ANEXO Nº 3

DECLARACIÓN JURADA DE CUMPLIMIENTO DE LOS TÉRMINOS DE REFERENCIA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº003-2024-SUNASS

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 MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE CIBERATAQUES PARA SERVIDORES DE MISIÓN CRÍTICA SOC AAS (CYBER SECURITY OPERATIONS CENTER)"**, 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

ANEXO Nº 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº003-2024-SUNASS

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 según el siguiente detalle:

El plazo máximo para la implementación del P01 es de hasta 30 días calendarios, contados desde el día siguiente de suscrito el contrato, dentro del cual se suscribirá el acta de inicio del servicio.

El plazo para la ejecución del servicio es de 36 meses contabilizados desde la fecha establecida en el acta de inicio del servicio.

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO Nº 5

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

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº003-2024-SUNASS

Presente.-

Los suscritos declaramos expresamente que hemos convenido en forma irrevocable, durante el lapso que dure el procedimiento de selección, para presentar una oferta conjunta al **CONCURSO PÚBLICO Nº003-2024-SUNASS.**

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] [%][27]

   [DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%][28]

   [DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

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

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

TOTAL OBLIGACIONES	100%[29]

[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.

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

ANEXO Nº 6

PRECIO DE LA OFERTA

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº003-2024-SUNASS

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
"SERVICIO DE MONITOREO, PREVENCIÓN, DETECCIÓN Y RESPUESTA ANTE CIBERATAQUES PARA SERVIDORES DE MISIÓN CRÍTICA SOC AAS (CYBER SECURITY OPERATIONS CENTER)".	
TOTAL	

El precio de la oferta en **SOLES** 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

- *En caso que el postor reduzca su oferta, según lo previsto en el artículo 68 del Reglamento, debe presentar nuevamente este Anexo.*

ANEXO Nº 8

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº003-2024-SUNASS

Presente.-

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

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [30]	FECHA DE LA CONFORMIDAD DE SER EL CASO[31]	EXPERIENCIA PROVENIENTE[32] DE:	MONEDA	IMPORTE[33]	TIPO DE CAMBIO VENTA[34]	MONTO FACTURADO ACUMULADO [35]
1										
2										
3										
4										

[30] 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.

[31] 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.

[32] 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"*.

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

[34] 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.

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

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP [30]	FECHA DE LA CONFORMIDAD DE SER EL CASO[31]	EXPERIENCIA PROVENIENTE[32] DE:	MONEDA	IMPORTE[33]	TIPO DE CAMBIO VENTA[34]	MONTO FACTURADO ACUMULADO [35]
5										
6										
7										
8										
9										
10										
	…									
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

ANEXO Nº 9

DECLARACIÓN JURADA
(NUMERAL 49.4 DEL ARTÍCULO 49 DEL REGLAMENTO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº003-2024-SUNASS

Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante
A efectos de cautelar la veracidad de esta declaración, el postor puede verificar la información de la Relación de Proveedores Sancionados por el Tribunal de Contrataciones del Estado con Sanción Vigente en http://portal.osce.gob.pe/rnp/content/relación-de-proveedores-sancionados. *También le asiste dicha facultad al órgano encargado de las contrataciones o al órgano de la Entidad al que se le haya asignado la función de verificación de la oferta presentada por el postor ganador de la buena pro.*

ANEXO N° 12

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

(DOCUMENTO A PRESENTAR EN EL PERFECCIONAMIENTO DEL CONTRATO)

Señores
COMITÉ DE SELECCIÓN
CONCURSO PÚBLICO Nº003-2024-SUNASS

Presente.-

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

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

[CONSIGNAR CIUDAD Y FECHA]

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

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