

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

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



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

SIMBOLOGÍA UTILIZADA:

N°	Símbolo	Descripción
1	[ABC] / [.....]	La información solicitada dentro de los corchetes sombreados debe ser completada por la Entidad durante la elaboración de las bases.
2	[ABC] / [.....]	Es una indicación, o información que deberá ser completada por la Entidad con posterioridad al otorgamiento de la buena pro para el caso específico de la elaboración de la PROFORMA DEL CONTRATO; o por los proveedores, en el caso de los ANEXOS de la oferta.
3	<div>Importante</div> <ul style="list-style-type: none"> • Abc 	Se refiere a consideraciones importantes a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda y por los proveedores.
4	<div>Advertencia</div> <ul style="list-style-type: none"> • Abc 	Se refiere a advertencias a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda y por los proveedores.
5	<div>Importante para la Entidad</div> <ul style="list-style-type: none"> • Xyz 	Se refiere a consideraciones importantes a tener en cuenta por el órgano encargado de las contrataciones o comité de selección, según corresponda y deben ser eliminadas una vez culminada la elaboración de las bases.

CARACTERÍSTICAS DEL DOCUMENTO:

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

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

INSTRUCCIONES DE USO:

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

Elaboradas en enero de 2019

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



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

**ADJUDICACIÓN SIMPLIFICADA N°
AS-043-2023-SAN GABAN S.A.**

(Primera Convocatoria)

BASES INTEGRADAS

CONTRATACIÓN DE

**“SERVICIO DE CIBERSEGURIDAD IT CON SEGURIDAD
ADMINISTRADA”**



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, así como el literal a) del artículo 89 del Reglamento.

Importante

No pueden formularse consultas ni observaciones respecto del contenido de una ficha de homologación aprobada. 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 el numeral 72.4 del artículo 72 del Reglamento y el literal a) del artículo 89 del Reglamento.

Importante

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

1.6. FORMA DE PRESENTACIÓN DE OFERTAS

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

Las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el postor (firma manuscrita o digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹). Los demás documentos deben ser visados por el postor. En el caso de persona jurídica, por su representante legal, apoderado o mandatario designado para dicho fin y, en el caso de persona natural, por este o su apoderado. No se acepta el pegado de la imagen de una firma o visto. Las ofertas se presentan foliadas.

Importante

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

1.7. PRESENTACIÓN Y APERTURA DE OFERTAS

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

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

Importante

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

En la apertura electrónica de la oferta, el órgano encargado de las contrataciones o el comité de selección, según corresponda, verifica la presentación de lo exigido en la sección específica

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>



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.

1.8. EVALUACIÓN DE LAS OFERTAS

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

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

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

Importante

En el caso de contratación de servicios en general que se presten fuera de la provincia de Lima y Callao, cuyo valor estimado no supere los doscientos mil Soles (S/ 200,000.00), a solicitud del postor se asigna una bonificación equivalente al diez por ciento (10%) sobre el puntaje total obtenido por los postores con domicilio en la provincia donde prestará el servicio, o en las provincias colindantes, sean o no pertenecientes al mismo departamento o región. El domicilio es el consignado en la constancia de inscripción ante el RNP². Lo mismo aplica en el caso de procedimientos de selección por relación de ítems, cuando algún ítem no supera el monto señalado anteriormente.

1.9. CALIFICACIÓN DE OFERTAS

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

1.10. SUBSANACIÓN DE LAS OFERTAS

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

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

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

1.11. RECHAZO DE LAS OFERTAS

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

De rechazarse alguna de las ofertas calificadas, el órgano encargado de las contrataciones o

² La constancia de inscripción electrónica se visualizará en el portal web del Registro Nacional de Proveedores www.mpp.gob.pe



el comité de selección, según corresponda, revisa el cumplimiento de los requisitos de calificación de los postores que siguen en el orden de prelación, en caso las hubiere.

1.12. OTORGAMIENTO DE LA BUENA PRO

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

1.13. CONSENTIMIENTO DE LA BUENA PRO

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

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

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

Importante

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



CAPÍTULO II

SOLUCIÓN DE CONTROVERSIAS DURANTE EL PROCEDIMIENTO DE SELECCIÓN

2.1. RECURSO DE APELACIÓN

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

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

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

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

Importante

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

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

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

2.2. PLAZOS DE INTERPOSICIÓN DEL RECURSO DE APELACIÓN

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

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



CAPÍTULO III DEL CONTRATO

3.1. PERFECCIONAMIENTO DEL CONTRATO

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

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

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

Importante

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

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

3.2. GARANTÍAS

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

3.2.1. GARANTÍA DE FIEL CUMPLIMIENTO

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

3.2.2. GARANTÍA DE FIEL CUMPLIMIENTO POR PRESTACIONES ACCESORIAS

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

Importante



- *En los contratos cuyos montos sean iguales o menores a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias. Dicha excepción también aplica a los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados no superen el monto señalado anteriormente, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.*
- *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 el 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 : Empresa de Generación Eléctrica San Gabán S.A. (San Gabán S.A.)

RUC N° : 20262221335

Domicilio legal : Av. Floral N° 245 – Barrio Bellavista – Puno

Teléfono: : 051-364401 anexos 4230 - 4231

Correo electrónico: : logistica@sangaban.com.pe

1.2. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación del “SERVICIO DE CIBERSEGURIDAD IT CON SEGURIDAD ADMINISTRADA”.

1.3. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado mediante Resolución de Gerencia General N° 300-2023/SAN GABAN SA del 01 de diciembre de 2023.

1.4. FUENTE DE FINANCIAMIENTO

Recursos Propios

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 se distribuirá la buena pro.

1.7. ALCANCES DEL REQUERIMIENTO

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

1.8. PLAZO DE PRESTACIÓN DEL SERVICIO

Los servicios materia de la presente convocatoria se prestarán en el plazo de setecientos treinta y uno (731) días calendarios 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 S/ 6.00 (seis con 00/100 soles) depositando dicho importe en nuestra cuenta en soles en el Banco Scotiabank a la Cuenta N° 000-0222097 y enviar el comprobante de depósito al correo electrónico logistica@sangaban.com.pe; el recojo de la copia de reproducción de las bases podrán hacerlos en Av. Floral N° 245 Barrio Bellavista – Puno, en caso de ubicarse fuera de la ciudad de Puno se podrán enviar la copia de las bases a la dirección que nos consignent con pago en destino por el envío.

Importante

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



1.10. BASE LEGAL

- Decreto Legislativo N° 1440 – Decreto Legislativo del Sistema Nacional de Presupuesto Público.
- Ley N° 31638 – Ley de Presupuesto del Sector Público para el Año Fiscal 2023.
- Ley N° 31639 – Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2023.
- Decreto Supremo N° 082-2019-EF que Aprueba el TUO de la Ley N° 30225 – Ley de Contrataciones del Estado.
- Decreto Supremo N° 344-2018-EF que Aprueba el Reglamento de la Ley N° 30225 - Ley de Contrataciones del Estado, modificado por Decretos Supremos N° 377-2019-EF, N° 168-2020-EF, N° 250-2020-EF y N° 162-2021-EF.
- Decreto Supremo N° 004-2019-JUS que Aprueba el TUO de la Ley N° 27444 – Ley del Procedimiento Administrativo General.
- Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y de Acceso a la Información Pública, aprobado por Decreto Supremo N° 043-2003-PCM.
- Código Civil.
- Directivas y Opiniones del OSCE.
- Cualquier otra disposición legal vigente que permita desarrollar el objeto de la convocatoria, que no contravenga lo regulado por la Ley de Contrataciones del Estado
- Directiva Gestión y proceso presupuestario de las entidades bajo el ámbito del FONAFE).
- Documentos de San Gabán S.A.: EGESG-D-G-80 (Política Anticorrupción): publicada en la WEB de SAN GABÁN S.A.: <http://www.sangaban.com.pe/index.aspx?seccion=9511>.

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 documentos³, la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta

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

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

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

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

- c) Declaración jurada de acuerdo con el literal b) del artículo 52 del Reglamento **(Anexo N°2)**
- d) Declaración jurada de cumplimiento de los Términos de Referencia contenidos en el numeral 3.1 del Capítulo III de la presente sección. **(Anexo N° 3)**
- e) Declaración jurada de plazo de prestación del servicio. **(Anexo N° 4)⁴**
- f) Promesa de consorcio con firmas legalizadas, de ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común y las obligaciones a las que se compromete cada uno de los integrantes del consorcio así como el porcentaje equivalente a dichas obligaciones. **(Anexo N° 5)**
- g) El precio de la oferta en SOLES. Adjuntar obligatoriamente el **Anexo N° 6**.

Importante

³ La omisión del índice no determina la no admisión de la oferta.

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.



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

2.2.1.2. Documentos para acreditar los requisitos de calificación

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

2.2.2. Documentación de presentación facultativa:

- a) En el caso de microempresas y pequeñas empresas integradas por personas con discapacidad, o en el caso de consorcios conformados en su totalidad por estas empresas, deben presentar la constancia o certificado con el cual acredite su inscripción en el Registro de Empresas Promocionales para Personas con Discapacidad⁵.
- b) Solicitud de bonificación por tener la condición de micro y pequeña empresa. (**Anexo N° 11**)

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 de corresponder.
- b) Contrato de consorcio con firmas legalizadas ante Notario de cada uno de los integrantes, de ser el caso.
- c) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y la entidad bancaria en el exterior.
- d) Copia de la vigencia del poder del representante legal de la empresa que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
- e) Copia de DNI del postor en caso de persona natural, o de su representante legal en caso de persona jurídica.
- f) Domicilio para efectos de la notificación durante la ejecución del contrato.
- g) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación ⁶. (**Anexo N° 12**).
- h) Detalle de los precios unitarios del precio ofertado⁷.

Importante

- *En caso que el postor ganador de la buena pro sea un consorcio, las garantías que presente este para el perfeccionamiento del contrato, así como durante la ejecución contractual, de ser el caso, además de cumplir con las condiciones establecidas en el artículo 33 de la Ley y en el artículo 148 del Reglamento, deben consignar expresamente el nombre completo o la denominación o razón social de los integrantes del consorcio, en calidad de garantizados, de lo contrario no podrán ser aceptadas por las Entidades. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio, conforme lo dispuesto en la Directiva Participación de Proveedores en Consorcio en las Contrataciones del Estado.*
- *En los contratos periódicos de prestación de servicios en general que celebren las Entidades con las micro y pequeñas empresas, estas últimas pueden otorgar como garantía de fiel cumplimiento el diez por ciento (10%) del monto del contrato, porcentaje que es retenido por*

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

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

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



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 y el 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 cuyos montos sean iguales o menores a doscientos mil Soles (S/ 200,000.00), no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias. Dicha excepción también aplica a los contratos derivados de procedimientos de selección por relación de ítems, cuando el monto del ítem adjudicado o la sumatoria de los montos de los ítems adjudicados no supere el monto señalado anteriormente, conforme a lo dispuesto en el literal a) del artículo 152 del Reglamento.

Importante

- Corresponde a la Entidad verificar que las garantías presentadas por el postor ganador de la buena pro cumplan con los requisitos y condiciones necesarios para su aceptación y eventual ejecución, sin perjuicio de la determinación de las responsabilidades funcionales que correspondan.
- De conformidad con el Reglamento Consular del Perú aprobado mediante Decreto Supremo N° 076-2005-RE para que los documentos públicos y privados extendidos en el exterior tengan validez en el Perú, deben estar legalizados por los funcionarios consulares peruanos y refrendados por el Ministerio de Relaciones Exteriores del Perú, salvo que se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, en cuyo caso bastará con que estos cuenten con la Apostilla de la Haya⁸.
- La Entidad no puede exigir documentación o información adicional a la consignada en el presente numeral para el perfeccionamiento del contrato.

2.4. PERFECCIONAMIENTO DEL CONTRATO

El contrato se perfecciona con la suscripción del documento que lo contiene. Para dicho efecto el postor ganador de la buena pro, dentro del plazo previsto en el artículo 141 del Reglamento, debe presentar la documentación requerida en la AV. FLORAL N° 245 BARRIO BELLAVISTA – PUNO o remitirla al correo electrónico mesadepartes@sangaban.com.pe y logística@sangaban.com.pe

Asimismo, para la suscripción del contrato el postor ganador deberá de concurrir a las instalaciones de San Gabán S.A. (AV. FLORAL N° 245 BARRIO BELLAVISTA – PUNO).

2.5. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista considerará el siguiente detalle:

Descripción	Requisitos
Primer pago: (VL) Valor del Licenciamiento	1. Incluye la instalación, configuración, despliegue, capacitación y todo aspecto con conlleve a la puesta en operación del producto o suite antimalware. Se emitirá un Acta de Recepción e Inicio del Servicio. 2. La conformidad de la Oficina de TIC.
Valorizaciones mensuales: (VS) Valor del servicio gestionado (12 pagos al final de	1, Previa presentación del informe mensual de la seguridad gestionada, los reportes de incidentes con los tiempos de atención



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

Descripción	Requisitos
cada mes) y 1 día antes del último día hábil del mes.	reales por cada ticket generado, y con las conclusiones y recomendaciones; tanto del NOC y del SOC. 2. La conformidad de la Oficina de TIC.

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

- Informe del funcionario responsable del Oficina de Tecnologías de la Información y Comunicaciones emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago (FACTURA ELECTRONICA y su archivo de extensión .xml).
- Carta o documento donde el contratista señala el número de cuenta corriente, CCI y nombre de la entidad bancaria, para el trámite pago.
- Informe mensual unificado.

Dicha documentación se debe presentar en Mesa de Partes Virtual San Gabán S.A. mesadepartes@sangaban.com.pe con copia a facturalogistica@sangaban.com.pe, si es físicamente será en la Sede Administrativa sito en Av. Floral 245, ciudad, distrito y departamento de Puno.

La Entidad debe pagar las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguientes a la conformidad, siempre que se haya verificado el cumplimiento de las condiciones establecidas en los TERMINOS DE REFERENCIA y el contrato.



CAPÍTULO III REQUERIMIENTO

3.1. TERMINOS DE REFERENCIA

Servicio de Ciberseguridad IT con Seguridad Administrada”

1. FINALIDAD PÚBLICA

Proveer las herramientas, el monitoreo y la gestión de incidentes de seguridad informática acorde con la política de seguridad de la información, alineada a la norma técnica peruana NTP ISO/IEC 27001:2022 EDI, el lineamiento de ciberseguridad de FONAFE, respecto a la identificación, protección, detección y respuesta en SAN GABÁN S.A. contra las amenazas y vulnerabilidades por malware, intrusión, secuestro para la mitigación de riesgos de seguridad de la información e informática.

2. OBJETIVO DE LA CONTRATACION

Se requiere adquirir el licenciamiento de la solución de ciberseguridad IT y el servicio de NOC (*Network Operations Center*) y SOC (*Security Operations Center*), referida a nuestra infraestructura tecnológica para la gestión y tratamiento de incidentes de ciberseguridad, en base al marco del estándar NIST para IT, de conformidad con los alcances expuestos en el numeral 8 de estos Términos de Referencia (TdR).

3. ANTECEDENTES DE LA CONTRATACIÓN

San Gabán S.A. cuenta con servicios cloud centralizados, denominados ePolicy Orchestrator y monitoreo EDR, que gestionan la ciberseguridad de todos los *endpoints* conectados a la red de datos, entendiéndose que se componen de: servidores, estaciones de trabajo, estaciones móviles (laptops y notebooks), tablets y celulares de plataforma Windows, Linux y Apple. Asimismo, cuenta con el servicio de seguridad actualizada y centralizada en tiempo real, sistema de reportes de incidentes de amenazas, explotación de vulnerabilidades, eventos y control del licenciamiento de cada producto según se requiera: antivirus, firewall, control web, control de medios removibles para equipos.

Actualmente está integrada con el Active Directory® de Microsoft Windows Server® 2019.

San Gabán S.A. ha implementado la Norma NTP ISO/IEC 27001, a través de un Sistema de Gestión de Seguridad de la Información y cuenta con una política de gestión que establece la aplicación de procedimientos y controles de seguridad, que la presente adquisición de herramientas debe coadyuvar a su implementación y mitigación de riesgos.

4. SISTEMA DE CONTRATACIÓN

Suma alzada.

5. ADELANTOS:

No aplican adelantos para esta contratación.

6. SUBCONTRATACIÓN

Es procedente que el Contratista subcontrate parte de las prestaciones a su cargo, el cual no podrá exceder del 40% del monto total del contrato original y/u orden según corresponda.

El CONTRATISTA mantiene la responsabilidad por la ejecución total de la contratación frente a la Entidad, asimismo, las obligaciones y responsabilidades derivadas de la subcontratación son ajenas a la Entidad.

7. REGLAMENTOS TÉCNICOS, NORMAS METROLÓGICAS Y/O SANITARIAS

No se incluyen normas obligatorias y/o voluntarias.

8. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

El servicio de ciberseguridad IT requiere contratar un proveedor de servicios que sea una persona natural o jurídica dedicada al rubro del objeto de la contratación con experiencia en la especialidad de ciberseguridad.

Debe ser representante, socio, distribuidor oficial o similar de la marca del fabricante de la solución del licenciamiento a proveer; para evidenciarlo deberá adjuntar carta y/o certificado y/o documento para perfeccionamiento del contrato.



8.1 LICENCIAMIENTO

El contratista deberá proporcionar licenciamiento para la solución de ciberseguridad con seguridad gestionada, según lo siguiente:

DESCRIPCION	CANT.	PLAZO DEL SERVICIO
Licenciamiento de solución de ciberseguridad	180	2 años

La solución debe contemplar las siguientes características básicas, descritas a continuación:

- Debe admitir arquitecturas de 32 bits y 64 bits
- Debe admitir las siguientes plataformas cliente:
 - Microsoft Windows 11, Windows 10, Windows 8.1 y Windows 8.
 - Microsoft Windows Server 2022, Windows Server 2019, Windows Server 2016 y Windows Server 2012.
 - macOS Big Sur 11.x, Catalina 10.15.x, Mojave 10.14.x, High Sierra 10.13.x, Sierra 10.12.x.
 - Red Hat Enterprise Linux, Oracle Linux 6.x y superior.
- Debe admitir la instalación de agente en los sistemas operativos anteriormente virtualizados en cualquier plataforma de virtualización.
- La protección debe ser realizada por medio de un software específico que atienda las funcionalidades descritas en el presente término de referencia y deberá contener un agente de gestión independiente al del software de protección, permitiendo que los componentes sean agregados o removidos conforme a las necesidades de los administradores.
- El conjunto de software de protección y agente de administración debe ser suministrado por el mismo fabricante.
- El software de protección debe comprender las siguientes características:
 - Prevención de amenazas.
 - Firewall y prevención de intrusos.
 - Control Web.
 - Prevención adaptable contra amenazas.
- Todas las funcionalidades deben ser gestionadas por una consola única con las capacidades mínimas de:
 - Reportes.
 - Dashboards.
 - Políticas.
 - Configuración.
 - Instalación/Desinstalación.
- El cliente debe ser capaz de operar en modo autónomo y permitir que las configuraciones se apliquen directamente en el cliente.
- El cliente debe ser capaz de actualizar la configuración para detectar amenazas, parches y revisiones desde un servidor definido por el administrador o directamente en los servidores del fabricante.
- La solución de prevención debe ser colaborativa, es decir, los módulos requeridos deben ser capaces de intercambiar información para un análisis contextual, no basado solamente en firmas de detección.
- La solución debe poseer múltiples capas de protección, no se aceptarán soluciones basadas sólo en firmas.
- La solución deberá realizar verificaciones periódicas en el ambiente para alertar al fabricante de posibles problemas ocasionados por la actualización de una vacuna.
- La solución debe contener un módulo capaz de proteger contra BOT nets, denegación de servicio, ejecutables no confiables y conexiones web malintencionadas.
- La solución debe contener un módulo capaz de garantizar una navegación web segura, previniendo contra sitios maliciosos, descargas de amenazas y garantizar la política de acceso (Permitir / Negar).
- La solución debe contener un módulo capaz de garantizar la integración entre las soluciones del fabricante propuesto y entre soluciones de terceros fabricantes (Ejemplo: Checkpoint, Fortinet,

AN GABAN S.A.
PRESIDENTE
DE SELECCIÓN

AN GABAN S.A.
MIEMBRO
DE SELECCIÓN

AN GABAN S.A.
MIEMBRO
COMITÉ DE SELECCIÓN

FireEye, NMAP, Cisco, IBM), compartiendo la información para una mejor mitigación de amenazas nuevas, este módulo debe ser público para su desarrollo abierto.

8.2 PROTECCIONES PARA WINDOWS

8.2.1 Prevención de explotación.

- Debe, como mínimo dos modos de protección (Ejemplo: Estándar / Máximo).
- Debe ser posible activar / desactivar la protección contra el escalamiento de privilegios.
- Debe ser posible habilitar / deshabilitar la prevención de ejecución de datos de Windows.
- Debe ser posible seleccionar entre las acciones de bloquear o bloquear e informar.
- Debe contener firmas contra ataques con contenido actualizable periódicamente.
- Debe contener la firma de ataques con contenido actualizable periódicamente.
- Debe permitir el bloqueo de amenazas y ataques de red.
- Debe permitir el monitoreo de ataques de *Buffer Overflow* en procesos y aplicaciones específicas.
- Debe ser posible configurar exclusiones. Ejemplo: por proceso, módulo invocador, otros.

8.2.2 Prevención de acceso.

Debe proporcionar reglas de protección de forma nativa, es decir, definidas por el fabricante de la solución como mínimo para:

- Acceso remoto a carpetas locales.
- Cambiar las políticas de derechos de usuario.
- Cambiar registros de extensión de archivo.
- Creación de nuevos archivos en la carpeta Archivo de programa.
- Creación de nuevos ejecutables en la carpeta de Windows.
- Crear / modificar de forma remota archivos ejecutables portátiles, archivos INI, PIF y ubicaciones del sistema.
- Crear o modificar de forma remota archivos o carpetas.
- Deshabilite el editor de registro y el administrador de tareas.
- Ejecuta archivos desde carpetas de usuario.
- Ejecución de script por el host de script de Windows.
- Instalar ayudas de navegación o extensiones de Shell.
- Instalar nuevos CLSID, APPID y TYPELIB.
- Modificar la configuración de red.
- Modificar la configuración de Internet Explorer.
- Modificar procesos centrales de Windows.
- Navegadores que inician programas desde la carpeta de descarga.
- Registrar programas para ejecución automática.

Las reglas especificadas permitirán el Bloqueo, Información, Bloqueo e información.

Debe permitir que el administrador cree reglas personalizadas con al menos los siguientes parámetros: Procesos, archivos, llaves de registro, valor de registro, servicios. Cada parámetro deberá tener opciones para configurar las reglas, ejemplos: Archivos (Crear, eliminar, ejecutar, lectura, etc.), servicios (Inicio, interrumpir, pausar, crear, quitar, etc.)

Debe permitir la creación de exclusiones.

8.2.3 Escaneo de acceso

- El análisis debe ser habilitado/desactivado por la opción del administrador.
- Debe iniciar la protección durante el inicio del sistema operativo.
- Debe ser capaz de realizar análisis en el sector de inicio.
- El administrador de la solución debe especificar el tiempo máximo de análisis para un único archivo.
- Debe revisar los procesos durante el inicio del servicio y la actualización de contenido.
- Debe permitir al administrador analizar instaladores de confianza.
- Debe realizar análisis durante la copia entre carpetas locales.
- La solución debe tener una conexión con el Centro de Inteligencia del fabricante, que puede ser activado o desactivado por el administrador.



- Debe permitir la configuración del nivel de agresividad del análisis en diferentes niveles.
- Debe permitir integración con la funcionalidad AMSI (*Antimalware Scan Interface*) de Microsoft.
- Debe permitir aplicar la configuración a todos los procesos del sistema operativo o a una lista específica creada por el administrador.
- Debe permitir en análisis cuando se produce lecturas y/o escrituras en disco y/o permitiendo que la solución misma tome la decisión de la técnica más adecuada.
- Debe permitir el análisis en unidades de red, archivos de backup, archivos comprimidos, archivos codificados (MIME).
- Debe detectar programas no deseados, amenazas en programas y amenazas desconocidos en macros.
- Debe permitir la creación de perfiles de análisis basados en una lista de procesos.
- Debe permitirle seleccionar al menos una de las siguientes opciones de acción después de detectar una amenaza: Limpiar, excluir, denegar acceso, otros.
- Debe permitirle seleccionar al menos una de las siguientes opciones de acción después de detectar un programa no deseado: Limpiar, excluir, permitir/denegar acceso, otros.
- Debe permitir al administrador administrar una lista de exclusiones.
- Debe tener módulo capaz de interceptar scripts destinados a *Windows Host Scripting* y analizarlo para indicar si es malicioso o no.
- Debe permitir la creación de listas de exclusión de URL que no sufrirán interceptación y análisis de script.
- Al detectar una amenaza, el agente debe emitir una notificación al usuario con un mensaje que el administrador de la solución pueda personalizar.

8.2.4 Análisis bajo demanda

- Debe ser posible realizar exploraciones programadas con periodicidad diaria o semanal:
 - Debe permitir la creación de una repetición de la tarea.
 - Debe permitirle establecer el tiempo de ejecución de la tarea de análisis.
 - Debe permitir la creación de la tarea de escaneo de con programación aleatoria.
- Debe permitir que los análisis programados se realicen después del inicio de sesión del usuario o durante el inicio del sistema operativo.
- Debe permitirle elegir (uno o más) los objetivos de la exploración, entre ellos:
 - Los sitios de exploración (memoria, procesos, archivos, unidades, etc.)
 - Los tipos de archivos que se analizarán
 - Opciones adicionales como la detección de programas no deseados, amenazas en programas y amenazas macro desconocidos.
 - Zonas de exclusión que no deben ser analizadas.
- Debe permitir la integración con el Centro de Inteligencia del fabricante durante el escaneo programado para la detección de amenazas desconocidas.
- Debe permitirle seleccionar al menos una de las siguientes opciones de acción después de detectar una amenaza: Limpiar, excluir, denegar, otros.
- Para minimizar el impacto en el usuario, la solución debe permitir:
 - El uso de la memoria caché, es decir, los archivos que ya han sido analizados y no han cambiado su contenido no serán reanalizados.
 - Comience a escanear solo cuando el sistema esté inactivo.
 - Permitir al usuario reanudar los análisis en pausa.
 - Limitar el porcentaje de CPU a ser utilizado por la tarea de análisis.
- Debe permitir que el administrador introduzca una cuenta de dominio para realizar el análisis de unidades de red.

8.2.5 Protección de amenazas para Linux

- Debe permitir la actualización automática de las vacunas de detección.
- Debe detectar amenazas utilizando métodos de acceso y escaneo a pedido.
- Debe permitir que los escaneos se realicen a través de la consola centralizada mediante tareas.
- Al detectar una amenaza, debe responder con al menos las siguientes acciones: Borrar, eliminar, denegar, otros.



- Debe permitir al administrador crear excepciones de escaneo, es decir, no permitir que la herramienta realice un escaneo en ciertas carpetas o archivos.
- Debe permitir la opción de mantener la configuración de eliminación realizada en el agente, no sobrescrita por la política principal.
- Debe permitir la administración del agente local a través de la línea de comando.
- Al configurar el análisis en acceso, debe permitir: Cuando analizar (ejemplo: al leer el archivo), qué analizar (ejemplo: todos los archivos).
- Análisis de archivos comprimidos, volumen de red, programas no deseados.
- Al configurar análisis bajo demanda, debe permitir análisis de: archivos comprimidos, PUP, macro desconocido, programa desconocido, rutas de análisis (ruta), carpetas y subcarpetas, macros.
- Eliminar rutas, carpetas y tipos de archivos.
- Debe tener cuarentena local para almacenar amenazas desconocidas.
- Debe tomar medidas para mover artefactos maliciosos al área de cuarentena.
- Debe usar la heurística para detectar archivos potencialmente maliciosos.
- Si se produce un tiempo de espera durante un análisis, debe permitir al administrador la configuración para permitir o denegar el acceso al archivo.

8.2.6 Protección de red

El módulo Firewall de Host debe incluir las siguientes capacidades:

- Debe permitir habilitar / deshabilitar el módulo de firewall desde la consola.
- Debe ser capaz de prevenir intrusiones y proteger los equipos asegurando la cobertura contra ataques de día cero.
- El firewall de Host debe permitir el bloqueo del tráfico entrante y el control del tráfico saliente
- Debe tener firmas de protección para: Archivos, llaves de registro, procesos, servicios
- Debe permitir el tráfico saliente solo después de iniciar los servicios de Firewall.
- Deber ser posible bloquear el tráfico *bridge*.
- Debe ser posible evitar ataques de *IP Spoofing*.
- El módulo debe permitir la creación de reglas de manera adaptativa, es decir, en una estación modelo definida por el administrador, debe poder crear las reglas automáticamente.
- Debe ser posible bloquear el tráfico de todos los procesos identificados como no confiables.
- Debe permitir la creación de una lista de procesos identificados como confiables utilizando la siguiente información como mínimo: Nombre, ruta, hash MD5, firma digital
- Debe permitir la integración con el propio centro de inteligencia del fabricante para bloquear las amenazas asociadas a conexiones maliciosas.
- Las conexiones identificadas por el Centro de inteligencia se pueden configurar mediante una reputación mínima para su bloqueo, por ejemplo, Riesgo alto o Riesgo medio.
- Debe ser posible obtener un registro de los eventos de conexiones bloqueadas y permitidas por el módulo.
- Debe permitir la inspección del protocolo FTP.
- Debe ser posible bloquear el tráfico de protocolos no compatibles.
- El módulo de Firewall debe venir con un conjunto de reglas previamente creadas por el propio fabricante.
- El módulo de firewall debe permitir la creación de reglas personalizadas, con al menos los siguientes parámetros: Acciones, dirección de la regla, protocolos. Los protocolos deben incluir: Cualquier protocolo, IP (ipv4, ipv6), tipo de conexión (cableado, wifi, virtual), especificación de red (IP, Subnet, FQDN), transporte (Todos, ICMP, TCP, UDP, STP, otros), programación (días de la semana, horas de inicio y fin), otros parámetros como aplicaciones u otros.
- Debe tener las siguientes protecciones como mínimo:
 - *Generic Buffer Overflow Protection.*
 - *Exploit Prevention.*
 - *Data Execution Protection.*
- Debe contar con un módulo de protección contra intrusiones en la red.
- El módulo de protección contra intrusiones debe tener reglas ya definidas por el fabricante.
- Debe permitir la creación personalizada de reglas de protección



- Al bloquear a un atacante en particular mediante el módulo de protección de red, será posible indicar un tiempo mínimo dentro del cual la máquina no podrá establecer sesiones con el atacante.
- Permitirá la exclusión de firmas y direcciones IP del mecanismo de análisis.
- Debe proporcionar protección para aplicaciones como Microsoft Office, Chrome, Edge, Acrobat.

8.2.7 Protección web

El módulo de Control web debe tener las siguientes funcionalidades:

- Debe permitir el bloqueo de navegadores no compatibles, entre ellos: Opera, Safari, otros.
- Debe permitir el control de los navegadores compatibles, incluidos: Chrome, Firefox, Edge, Edge Chromium.
- Debe poder usar la lista de categorías para bloquear sitios relacionados con contenido no autorizado.
- Debe ser posible bloquear un sitio de acuerdo con su calificación: Riesgo alto, medio, no categorizado.
- Debe ser posible bloquear un sitio que nunca ha sido analizado por el centro de inteligencia del fabricante.
- Debe ser posible bloquear las páginas de phishing incluso si el acceso al contenido se encuentra permitido.
- Debe permitir el escaneo de archivos descargados de internet.
- Debe ser posible excluir las direcciones IP del escaneo.
- Debe permitir la búsqueda segura de buscadores, entre ellos: Google, Yahoo, Bing, otros.
- Debería bloquear enlaces a sitios de alto riesgo.
- Debe permitir la personalización de los mensajes presentados al usuario.

8.2.8 Protección adaptativa de amenazas

El módulo de inteligencia de amenazas debe contener los siguientes mecanismos:

- a) Contención dinámica de aplicaciones:
- La solución debe permitir la contención dinámica de aplicaciones y archivos ejecutables con características maliciosas (Ejemplo: ransomware)
 - La solución debe ser capaz de evaluar aplicaciones desconocidas y potencialmente maliciosas en un entorno controlado.
 - Debe permitirle indicar aplicaciones confiables para que no caigan en el filtro de contención dinámica.
 - No debe requerir conexión al centro de inteligencia del fabricante para que la protección se active o ejecute.
 - La solución debe mantener una caché de reputación local con información de la aplicación – conocida, desconocida y maliciosa.
 - Debe ser posible ordenar cada aplicación manualmente e incluso su reclasificación a través de la consola de administración central
 - Bloquear comportamientos maliciosos como:
 - Acceso local desde cookies.
 - Creación de archivos a partir de archivos con .bat, .exe, .html, .vbs, otros
 - Creación de archivos en cualquier lugar de la red
 - Creación de nuevos CLSID, APPIDs y TYPELIBs
 - Bloquear la desactivación de ejecutables críticos del sistema operativo
 - Leer/Eliminar/Escribir Archivos dirigidos por ransomware
 - Escribir y leer en memoria de otro proceso
 - Bloqueo de modificación de directiva de firewall de Windows
 - Bloqueo de modificación de carpetas de tareas de Windows
 - Bloqueo de modificación de archivos críticos de Windows y ubicaciones del registro.
 - Bloqueo de modificación de bits de atributos.
 - Bloqueo de la suspensión de un proceso
 - Bloqueo de terminación de otro proceso
 - Otros bloqueos.



- A partir de los comportamientos observados, debe ser posible bloquear o sólo informar si ocurre
 - Debe ser capaz de informar al usuario de las amenazas encontradas a través de mensajes personalizados
 - Modo de activación de bloqueo dinámico para cualquier archivo desconocido al que acceda el sistema operativo y nunca visto por la solución
 - Debe ser posible asignar la regla de acuerdo con una política equilibrada, con el objetivo de una mayor seguridad o productividad del usuario
 - La protección debe estar contenida en el mismo agente de protección, sin requerir otro software o aplicación adicional en la estación de trabajo para la ejecución y activación de la protección
- b) Módulo de Análisis Avanzado
- Debe permitir el análisis de los procesos iniciados en unidades asignadas a la red.
 - Debe ser capaz de trabajar con técnicas de análisis matemático para identificar amenazas sin necesidad de firmas.
 - Al seleccionar el análisis sólo en el cliente, debe ser posible indicar la sensibilidad del motor de análisis.
 - Debe permitir la selección del mejor modo de operación de la solución en base a recomendaciones del fabricante de ambientes de trabajo.
 - Debe activar el módulo de contención dinámica automáticamente si una amenaza alcanza un cierto nivel de criticidad que debe indicar el administrador de la solución.
- c) Reputación local de amenazas
- El módulo de reputación local debe mantener una base de datos con todos los ejecutables detectados en el entorno.
 - Para cada ejecutable, las reputaciones deben mostrarse utilizando diferentes técnicas, tanto como parte de técnicas del mismo fabricante como en interacción con terceros.
 - Debe ser capaz de informar la URL de origen del archivo y su reputación.
 - Debe permitir la identificación de la estación de trabajo y el usuario asociado con el mismo.
 - El módulo debe permitir la automatización de contramedidas de soluciones del mismo fabricante y de terceros fabricantes.

8.3 Características adicionales de la plataforma de ciberseguridad

8.3.1 Control de dispositivos removibles

Mantener la productividad operativa. - bloqueo basado en hardware, en cualquier dispositivo de almacenamiento extraíble; asegurar de que los empleados siguen usando de forma segura los dispositivos permitidos como parte de sus actividades laborales diarias.

Gestión integral de dispositivos y datos. - Que regule el uso por parte de sus empleados de unidades USB, dispositivos Bluetooth e infrarrojos, cámaras fotográficas, equipos de imagen, puertos COM y LPT.

Controles diferenciados. - Que especifique qué dispositivos se pueden usar y cuáles no en función de cualquier parámetro de dispositivo de Windows, como identificación de producto, identificación de proveedor, número de serie, clase de dispositivo y nombre de dispositivo; para los dispositivos que se pueden usar.

Administración centralizada. - Que defina, despliegue, administre y actualice centralmente las directivas y agentes de seguridad en todo su entorno; establezca directivas de dispositivos por usuario, grupo o departamento.

8.3.2 Control de Aplicaciones

- Reducir los riesgos asociados a las aplicaciones no autorizadas para controlar los *Endpoints*, servidores y dispositivos fijos. Las amenazas persistentes avanzadas ejecutadas mediante ataques remotos o ingeniería social complican cada vez más la protección de SINEACE.
- Ayudar a burlar a los ciberdelincuentes y garantizar la seguridad y la productividad.
- Mediante el uso de un modelo de confianza dinámico y de innovadoras funciones de seguridad, como la inteligencia de reputación local y global, los análisis de comportamiento en tiempo real y la inmunización automática de los *endpoints*, esta solución deberá frustrar de manera



inmediata las amenazas persistentes avanzadas, sin necesidad de emplear las complicadas administraciones de listas ni las actualizaciones de firmas.

- Solución para proteger de las amenazas de tipo *zero-day*, prevenir los ataques de tipo *zero-day* y de amenazas persistentes avanzadas mediante el bloqueo de la ejecución de las aplicaciones no autorizadas.
- Función de inventariado que permita localizar y gestionar los archivos de aplicaciones. Agrupar todos los binarios (EXE, DLL, controladores y secuencias de comandos) por aplicación y proveedor, y mostrar en un formato jerárquico intuitivo clasificándolos de forma inteligente como aplicaciones bien conocidas, conocidas y poco conocidas.
- Mediante el uso de listas blancas, podrá evitar ataques de malware desconocido permitiendo la ejecución únicamente de aplicaciones bien conocidas de la lista blanca.
- En un momento en el que los usuarios demandan más flexibilidad para utilizar las aplicaciones en el entorno empresarial a través de la nube y las redes sociales, la solución permitirá tres opciones para potenciar la estrategia de lista blanca con el fin de mejorar la prevención de amenazas.
- Control eficaz del acceso a las aplicaciones con el software, una plataforma centralizada para la administración de las soluciones de seguridad.
- Reducción de los ciclos de aplicación de parches gracias a listas blancas seguras y a la protección avanzada de la memoria.

8.3.3 Consola de administración

- La gestión debe ser centralizada y soportar todos los módulos ofertados en una única consola de administración.
- La solución debe permitir ser implementada tanto on-premise como SaaS (Software as a Service), permitiendo elegir cual modalidad se desea utilizar (incluso ambas al tiempo) y sin incurrir en costos adicionales.
- La consola de administración on-premise debe admitir la instalación en los siguientes sistemas operativos como mínimo: Windows Server 2012 al 2019.
- Debe admitir la instalación en Microsoft Cluster.
- Debe ser compatible con Ipv4 e Ipv6.
- Debe admitir la virtualización del sistema operativo en cualquier plataforma de virtualización.
- Debe ser compatible mínimo con la base de datos SQL Server 2012 o superior.
- La consola de administración debe ser accesible a través de los principales navegadores.
- Debe ser posible la implementación de: Servidor de consola central, Base de Datos, interacción con agentes, así como Agentes distribuidores de actualizaciones.

8.3.4 Capacidades de Gestión

Debe tener un menú que permita al administrador ver las características de:

- Gestión de informes.
- Gestión de Sistemas.
- Gestión de políticas y configuraciones de productos enumeradas en este término de referencia.
- Gestión de software gestionado.
- Gestión de automatización.
- Gestión de Usuarios.
- Gestión de la configuración.
- Debe permitir al administrador la visibilidad del entorno a través de los paneles existentes en la solución.
- Debe permitir que el administrador cree, edite, importe y exporte dashboards.
- Debe permitir la creación de nuevos dashboards.
- La solución debe mostrar la consulta SQL realizada para la presentación de un panel.
- Debe permitir la exportación de los datos presentados a un dashboard que contenga sólo un resumen ejecutivo o el resumen más la colección completa de los datos.
- Debe permitirle exportar los datos al menos en formatos CSV, XML, HTML y PDF.
- Debe permitir al administrador crear informes a través de una sección en la consola de gestión que permita, adicionalmente, la personalización del formato del informe.
- Debe permitir al administrador el uso de queries para la construcción de los reportes.



- Al instalar el nuevo agente, debe ser redirigido automáticamente al grupo al cual debe pertenecer.
- La creación de grupos puede ser de manera personalizada o a través de la integración con Active Directory.
- Al ordenar a través del uso de IP Addressing, debe permitir el uso de una sola dirección, un rango IPV4/IPV6 y subred;
- Para permitir la detección de máquinas sin agente, mediante el uso de sensores que permitan identificar máquinas sin agente.
- Al identificar una máquina sin agente, la solución debe permitir la creación automatizada de respuestas, lo que permite que la instalación se realice de forma silenciosa para el usuario
- Debe permitir la adición manual de sistemas no gestionados, permitiendo la posterior instalación del agente.
- Permitir cambiar las directivas de los módulos de solución en los clientes de forma remota
- Debe permitir modificar las políticas en un único agente.
- Debe contar con una consola de gestión única que permita gestionar las características de seguridad y de agente tanto en estaciones de trabajo como en servidores.
- Permitir la actualización incremental de la lista de definiciones de virus en los clientes desde un único punto de la red local.
- Debe permitir la creación de una lista de repositorios que los clientes deben buscar por orden de prioridad.
- Debe permitir la creación de un grupo de pruebas para la aplicación de la vacuna antes de replicarlo en todos los equipos del ambiente.
- La solución debe permitir el uso de repositorios distribuidos para la distribución de software, vacunas y actualizaciones y parches.
- Los repositorios distribuidos deben sincronizarse con el repositorio central.
- En caso de indisponibilidad del repositorio central, debería poder configurar un repositorio de copia de seguridad en el que los repositorios vayan por actualizaciones.
- Debe permitir la creación de agentes locales con privilegios de distribución de actualizaciones
- Debe tener la funcionalidad de "lazy caching", es decir, descargar el repositorio principal, sólo cuando lo solicite algún otro agente.
- La solución debe permitir la instalación de agentes de replicación adicionales, responsables de la comunicación entre el agente de servidor, lo que permite la entrega de directivas y actualizaciones de la solución.
- Debe permitir la instalación de agentes de replicación en la DMZ.
- Debe permitir al administrador visualizar las características básicas de hardware de las máquinas.
- Debe permitir la creación de propiedades personalizadas, por ejemplo, informar al modelo de tarjeta de vídeo en una propiedad personalizada.
- Permitir el almacenamiento de la información recopilada de los clientes en una base de datos centralizada.
- Permitir diferentes niveles de administración del servidor, independientemente del inicio de sesión de red.
- Debe permitir la creación de políticas personalizadas.
- Debe presentar al administrador un historial de cambios de directiva para cada uno de los módulos de solución.
- Debe crear reglas de aplicación de directivas automatizadas basadas en la estación de trabajo o el usuario.
- Para la directiva basada en el usuario, debe poder crear al menos directivas diferenciadas para los módulos Firewall de host y Filtro web.
- Debe permitir la creación automatizada de respuestas al detectar eventos de amenaza, ya sea cliente o servidor.
- Soporte multiusuario, con diferentes niveles de acceso y permisos a productos gestionados
- Forzar el conjunto determinado en el servidor para los clientes.
- Si el cliente cambia la configuración, debe volver al valor predeterminado establecido en el servidor cuando es verificado por el agente.
- La comunicación entre los equipos cliente y el servidor de administración debe ser segura
- Informes que muestren lo siguiente:



- Máquinas con lista de definiciones de virus obsoletas;
 - ¿Qué versión del software (incluida la versión administrada en la nube) está instalada en cada máquina;
 - Los virus más detectados;
 - Las máquinas que más infecciones han sufrido en un período determinado;
 - Usuarios que han sufrido más infecciones en un período de tiempo determinado;
- Debe ser capaz de identificar y mostrar la visibilidad en qué estaciones han ejecutado un archivo (ejecutable) determinado.
- Debe ser capaz de identificar el archivo y bloquearlo en función de los criterios de reputación y riesgo.
- Gestione la actualización antivirus en portátiles automáticamente conectándose a una red local o remota.
- Apoyar el uso de múltiples repositorios para la actualización de productos y archivos de vacunas con replicación selectiva.
- Tener la capacidad de generar registros/registros para la auditoría.
- La solución de gestión debe tener la capacidad de etiquetar máquinas, facilitando así la distribución automática dentro de los grupos jerárquicos en la estructura de gestión.

8.3.5 Inteligencia de amenazas

- Debe contar con un módulo de inteligencia de amenazas que permita identificar las amenazas a nivel mundial filtrando tanto por sector, país, última detección, nombre, severidad, prevalencia.
- Dicha fuente de inteligencia debe utilizar la información obtenida por diferentes sensores y análisis utilizando *machine learning*.
- La solución deberá informar adecuadamente el nivel de protección de los dispositivos de la organización contra una amenaza/campaña específica permitiendo priorizar las actividades de remediación.
- La solución deberá brindar un análisis de postura de seguridad de la organización tanto en los vectores y nube en caso de contar con los adecuados elementos integrables.
- Debe permitir la generación de reportes de la postura de seguridad y dispositivos con cobertura insuficiente, eventos de detección de campañas tanto en PDF como CSV.
- Debe brindar información sobre los IoC detectados y asociados a una determinada campaña, permitiendo identificar si han estado presentes en algún dispositivo protegido en la organización.
- Dicha información de IoC debe permitir el inicio de actividades de respuesta mediante un módulo de detección y reacción (EDR).
- La información de IoC debe permitir ser exportada en formato json para ser utilizada libremente por parte de la organización.
- El análisis de una campaña de amenaza debe proveer información tal como descripción de la campaña, prevalencia global, sectores impactados, productos que mayormente la han detectado, indicadores analizados.
- Adicional a lo anterior, debe proveer un análisis del comportamiento identificado por la campaña, utilizando la matriz de MITRE para categorizar las técnicas observadas.
- Con el objetivo de facilitar las capacidades de prevención, debe brindar en listado de tácticas para prevenir, mitigar y medir el impacto de una amenaza determinada. La información debe ser útil para poder ser aplicada antes, durante y después de un ataque para prevenir de forma efectiva una amenaza.
- Para amenazas donde se hayan generado reglas de detección, debe ser posible exportarlas como reglas expertas, reglas sigma, reglas Yara y reglas de Snort.

8.3.6 Protección para Dispositivos Móviles

- Debe ofrecer protección en el dispositivo y en tiempo real para detectar las amenazas y proteger frente a ataques de tipo *zero-day*.
- La protección de red debe detectar si los dispositivos móviles se conectan a una red no segura o peligrosa.
- Debe instalarse directamente en los dispositivos móviles para proporcionar protección continua sin importar el modo de conexión del dispositivo móvil o incluso si está desconectado.

- Protección *anti-phishing* mediante la detección de enlaces peligrosos en mensajes de texto, apps de medios sociales y mensajes de correo electrónico.
- Debe poder interactuar con la solución de MDM Windows Intune para obtener datos principales de los móviles y aplicar soluciones a las amenazas y vulnerabilidades detectadas.
- Proteger los dispositivos móviles, proporcionando una completa solución de seguridad
- Capacidad para identificar y asignar directivas a Smartphones y Tablets.
- Análisis de seguridad a las aplicaciones móviles, protección frente al malware y notificación del cumplimiento de normativas.
- Deberá integrarse con la consola de administración, permitiendo -en términos de seguridad- la visualización de eventos y estado de los dispositivos gestionados, con el objetivo de facilitar el cumplimiento de normativas.
- Configurar correctamente los dispositivos móviles de acuerdo con las directivas de seguridad corporativas e imponer el cumplimiento de las normativas antes de que accedan a la red
- La implementación podrá realizarse utilizando una consola diferente a la Consola de Administración Centralizada, pero la solución deberá ser del mismo fabricante.

8.3.7 EDR (Endpoint Detection and Response)

- La solución debe permitir poner en cuarentena a los hosts comprometidos con el objetivo evitar movimientos laterales de códigos maliciosos.
- La solución debe permitir detener y/o eliminar un proceso en ejecución o persistente en las estaciones de trabajo.
- La solución ofertada debe permitir la segmentación de políticas para la operación de la plataforma, es decir, la herramienta debe permitir aplicar distintos tipos de políticas para un mismo ecosistema cliente.
- La solución debe permitir mecanismo de contención remotos en el *endpoint*.
- La solución debe permitir mecanismos de remediación remotos en el *endpoint*.
- La solución debe estar en capacidad de coleccionar información de procesos en ejecución.
- La solución debe estar en capacidad de coleccionar información de conexiones activas de red.
- La solución debe ser capaz de recolectar información de servicios que se ejecutan en el *endpoint*.
- La solución debe ser capaz de recolectar información de las tareas programadas en el *endpoint*.
- La solución debe ser capaz de coleccionar información histórica de navegación web y descargas.
- La solución debe coleccionar información del *filesystem*.
- La solución debe coleccionar logs de eventos.
- La solución debe tener la capacidad de eliminar/modificar llaves de registro.
- La solución debe permitir eliminar archivos remotamente.
- La solución debe permitir ejecutar *scrip* de manera arbitraria.
- La solución debe tener la capacidad de desinstalar programas de manera remota.
- La solución debe ser capaz de alertar un incidente en un tiempo muy cercano al tiempo real
- La solución debe llevar el proceso de investigación a minutos.
- La solución debe tener la capacidad de recolectar una imagen full de la memoria
- La solución debe coleccionar información de *Bash/Shell* históricamente
- La solución debe tener cobertura sobre TTPs descritos en *Mitre Att&ck Framework*.
- La solución debe permitir la creación de colectores de información de manera personalizada para realizar búsquedas en tiempo real y en proceso de *hunting*
- La solución debe permitir la creación de reacciones de manera personalizada para contener y aplicar remediaciones que se ajusten a las necesidades de la organización.
- La solución debe permitir soportar la creación de script de ejecución en Python, VBScript y/o *batch* ejecución de comandos de sistemas operativos de manera remota.

8.3.8 Reportes y administración.

- La solución debe contar con un panel de visualización de métricas de uso de la plataforma.
- La solución debe permitir la creación de distintos roles de usuarios dentro de la consola de gestión para el perfilamiento de usuarios.
- La herramienta debe permitir la vinculación de procesos mediante mecanismos de trace.
- La solución ofertada debe permitir la visualización de información en distintos modelos, desde vistas graficas de los hallazgos hasta el detalle de la información recolectada.



- La herramienta debe permitir la visualización de los hallazgos mediante vistas graficas.
- La herramienta debe permitir visualizar eventos históricos.

8.3.9 Integración

- La solución debe poseer integración con una herramienta para la gestión de políticas y despliegue ya sea en la nube o desplegada *on-premise*.
- La solución ofertada debe poder integrarse con diferentes soluciones de correlación.

8.4 SERVICIO DE OPERACIÓN DE LA SOLUCIÓN DE CIBERSEGURIDAD

El servicio de operación de la seguridad es un servicio que ejecutará cotidianamente acciones proactivas y reactivas con el objetivo de disminuir el riesgo y mantener o elevar el nivel de seguridad de la plataforma de San Gabán. Este servicio actuará en base a tres elementos:

- A. La visión, objetivos y metas de seguridad informática de San Gabán.
- B. La estrategia de seguridad propuesta por el contratista.
- C. El análisis de riesgo periódico que se ejecuta durante el servicio.

El contratista cumplirá labores cotidianas de atención y maniobras sobre la plataforma e incidentes de seguridad de EGE San Gabán. Este servicio realizará acciones técnicas a cargo de especialistas certificados y actuarán en base a metodologías modernas. Este servicio permitirá minimizar los incidentes de pérdida de información o de disponibilidad de los recursos informáticos, previniendo daños ocasionados por el software malicioso, la navegación insegura, las intrusiones, intentos de robo de información entre otras amenazas.

8.4.1 Objetivos del servicio

El objetivo principal del servicio es que las maniobras cotidianas y a demanda sean técnicamente eficientes y se apoyen en un estudio periódico y visión proactiva, de tal forma que se busque la mejora continua en el nivel de seguridad y la consecuente minimización del riesgo.

Otros objetivos del servicio:

- Supervisar el licenciamiento en un modelo corporativo y con representatividad ante el fabricante.
- Optimizar la arquitectura actual y el modelo de supervisión, aplicando las mejores prácticas del mercado.
- Mejorar la operación y eficiencia en las plataformas tecnológicas.
- Gestionar la plataforma y tomar acción oportuna ante amenazas externas e internas, minimizando los tiempos de afectación de los recursos operativos.
- Realizar un análisis de riesgo continuo, con el objetivo de buscar periódicamente la mejora continua y así hacer más eficientes y seguras las plataformas administradas.
- Establecer un modelo de mejora continua basado en indicadores periódicos.

8.4.2 Modalidad de servicio

Este servicio se brindará en la modalidad Off-Site con las facilidades:

- Gestor y/o operador.
- Equipo NOC que actuará en el horario de oficina de San Gabán.
- Equipo NOC actuará fuera del horario de oficina de San Gabán
- El servicio no se verá afectado en caso de inasistencias del personal.
- Personal se integra a procesos y cultura de San Gabán.

8.4.3 Metodología de trabajo

La metodología de servicio consistirá en seguir los fundamentos de un Sistema de Gestión de Seguridad, que ayudará a implementar y mantener total o parcialmente los requisitos, líneas guía y técnicas necesarias en los sistemas de seguridad.

Las normativas nacionales e internacionales relacionadas a la operación de seguridad deben ser:

- ISO/IEC 27001. Lineamientos guía y principios generales para iniciar, implementar, mantener un sistema de gestión de la seguridad de la información en una organización.
- ISO/IEC 27002. Mejores prácticas para los controles de seguridad de la información.
- ISO/IEC 31000. Principios y lineamientos guía de la gestión de riesgos.



Adicionalmente a las mencionadas, las prácticas relacionadas al análisis de riesgo contemplarán marcos metodológicos como NIST 800-39 / 800-37 / 800-30, ISO 27005 y FAIR.

8.4.4 Ámbito del servicio

El ámbito del servicio está circunscrito a la siguiente plataforma y componentes:

PLATAFORMA
Licenciamiento de solución de ciberseguridad

8.5 Actividades del Servicio

Las actividades que forman parte de este servicio deberán ser las siguientes:

8.5.1 Operación de la seguridad

i. Gestión de la seguridad

Desarrollará las siguientes actividades:

- Administración de la configuración idónea del sistema central y componentes distribuidos.
- Implantación de versiones y configuraciones.
- Administración de repositorios y bases de datos de información.
- Revisión cotidiana de la plataforma a cargo de un gestor de servicio
- Reporte de actualizaciones, cobertura y de cumplimiento de estándares de la plataforma.
- Supervisión de licenciamiento y suscripciones.
- Actualización del inventario de la plataforma operada.
- Gestión de perfiles y accesos de supervisión a plataforma operada.

ii. Cambios, configuraciones y maniobras

Este servicio recibirá, evaluará, aprobará e implementará las solicitudes de cambio y configuración para las plataformas de Firewall y Antimalware y mediante procedimientos establecidos. Estas solicitudes serán registradas, documentadas y supervisadas hasta su resolución y reporte, mediante procedimientos preestablecidos.

iii. Soporte técnico

Tendrá por objetivo absolver consultas técnicas y dar soporte a incidentes. Los incidentes o solicitudes serán recibidos y procesados hasta su completa resolución. Los incidentes atendidos serán registrados, tendrán seguimiento y a su finalización generarán el informe técnico respectivo. Incluirá maniobras en la modalidad Off-Site.

iv. Copias de respaldo de los sistemas de gestión

Consistirá en obtener periódicamente y almacenar de forma encriptada el respaldo de la configuración y de las políticas de seguridad de los sistemas de Ciberseguridad, a través de procedimientos aprobados de obtención, almacenamiento y restauración. De esta forma la plataforma estará preparada para recuperarse ante un posible desastre.

v. Gestión de las actualizaciones y mejoras

Se trata de la evaluación, planificación e instalación de mejoras y/o de nuevas versiones de los componentes administrados. Para este fin se evaluarán las últimas versiones y parches que sean publicadas por el fabricante ESET. Además, se evaluarán las versiones actuales, la oportunidad de mejora y los tiempos de fin de vida y de fin de soporte de cada una de ellas. De esta forma la UPSJB mantendrá su sistema siempre actualizado y protegido.

8.5.2 Planificación de la seguridad

Se realizarán las siguientes actividades de evaluación y planificación que permitan lograr efectividad y mejora continua en los mecanismos de seguridad implantados y administrados:

i. Comité de la Seguridad mensual

- ✓ Reportar indicadores.
- ✓ Reportar incidentes.
- ✓ Seguimiento de las iniciativas de seguridad.
- ✓ Tablero de mejora continua de seguridad.

8.5.3 Servicio de CyberSOC

Tendrá el siguiente alcance:

8.5.3.1 Monitoreo de salud de la plataforma



- ✓ Seguimiento de parámetros esenciales de salud y reporte del comportamiento de la plataforma que forma parte del alcance y sus elementos críticos, en aspectos como:
- ✓ Disponibilidad de sistema
- ✓ Nivel de procesamiento y memoria
- ✓ Múltiples niveles de alertas
- ✓ Actividad relevante para la seguridad y monitoreo SOC
- ✓ Comunicaciones: Enlaces VPN, interconexión con monitoreo.

Los parámetros se recogerán en un sistema central, el cual permitirá la monitorización, generación de informes y alertas mediante medios preestablecidos.

8.5.3.2 Monitoreo avanzado tiempo real y correlación de eventos de seguridad

Compilación y normalización de telemetría e indicadores técnicos obtenidos desde los sistemas que conforman el alcance del monitoreo. Ésta big data se reunirá y analizará en un sistema central SIEM (Security Information and Event Management) que permitirá la monitorización, previsión y seguimiento de incidentes, el almacenamiento de los eventos en base de datos y su explotación mediante consultas e informes.

Los mencionados indicadores y telemetría de seguridad aportarán información sobre comunicaciones, endpoints, identidades de usuario, cuentas privilegiadas, contenido, aplicaciones, cloud e infraestructura diversa, con el objetivo de generar alertas de seguridad predictiva y reversa. También se generan alertas de comportamiento sospechoso o malicioso que pueden convertirse en casos de seguridad que merezcan atención.

El contratista debe tener implementado en el CyberSOC sistemas modernos de XDR que generan telemetría que facilitan la analítica y la respuesta posterior del CyberSOC para mitigar las amenazas de forma inteligente con herramientas basadas en la inteligencia artificial y con acciones de los analistas.

8.5.3.3 Inteligencia de Ciberseguridad - Cyber Threat Intelligence

La inteligencia de ciberamenazas (Cyber Threat Intelligence) permitirá que el CyberSOC sea uno de los más avanzados, al recibir información global y permanente en forma de flujos de datos, indicadores de compromiso y de reportes de inteligencia, respecto a amenazas actuales.

El CyberSOC del contratista actuará de forma proactiva, estando al tanto de las amenazas que se orquestan a nivel global y agregando capacidad de detección técnica, logrando así que los sistemas monitoreados puedan estar mejor preparados para detectar y responder ante amenazas. Poseerá la capacidad de informarnos y de alertar sobre amenazas respecto a redes TI y redes OT (industriales), así como en segmentos específicos de mercado.

En suma, la Inteligencia de ciberamenazas conformará una ventaja preventiva en materia de información relevante, detección de seguridad, Hunting y análisis de casos.

8.5.3.4 Inteligencia en la Darknet (Darknet Intelligence)

El CyberSOC debe contar con el acceso a una base de datos con el cual los especialistas en inteligencia realizarán búsquedas en la Darknet profunda y redes relacionadas (Contenido Darknet, Contenido Deepweb, Plataformas de chat encriptado (Telegram y otros), Hacker fóruns, FTP servers, Marketplaces y otros lugares no divulgados) para encontrar indicios o evidencias de amenazas existentes o emergentes que puedan atentar contra EGE San Gabán.

8.5.3.5 Threat Hunting

Serán labores realizadas por analistas expertos del contratista, que permitirán examinar y catalogar amenazas avanzadas en base a tus tácticas, técnicas y procedimientos (TTPs) de ataque en la infraestructura.

Ciertas amenazas activas o pasivas no son detectadas por los controles de seguridad automatizados de prevención-detección y requieren un esfuerzo de Threat Hunting para

generar la inteligencia de seguridad, catalogación en matrices MITRE ATT&CK e identificación de los actores maliciosos.

8.5.3.6 Computer Security and Incident Response Team (CSIRT)

Serán las labores reactivas que efectúe el CyberSOC con el objetivo de actuar oportunamente, generar recomendaciones probadas y brindar asesoría de mitigación de incidentes puntuales o de gran escala. La respuesta avanzada a incidentes responderá metódicamente y seguirá un ciclo de acción, utilizando herramientas, librerías y normatividad como NIST SP 800-61 e ISO 27032.

La Respuesta Avanzada a Incidentes podrá ser activada en los siguientes casos:

- Por una ocurrencia en el site de San Gabán.
- A solicitud sustentada de San Gabán.
- Alerta preventiva en el sistema de correlación – SIEM.
- Acciones de iniciativa propia del contratista (Ejemplo durante el análisis de riesgo).

Consistirá en atender las emergencias causadas por amenazas de seguridad complejas como ataques, comportamiento malicioso o malware. Se encargarán de investigar el hecho con sus expertos acreditados, analizarán los activos informáticos afectados con una diversidad de herramientas especializadas, y plantearemos las acciones de mitigación, contención o remediación recomendadas para este hecho.

8.5.3.7 Alerta Temprana

Este servicio alertará de acuerdo con los procedimientos establecidos y de forma oportuna, ante amenazas o casos de seguridad que requieran atención. El equipo de especialistas del contratista se pondrá en contacto mediante medios preestablecidos para informar sobre las alertas preventivas y reactivas generadas.

Las alertas pueden ser emitidas por medios electrónicos o por voz y luego complementadas.

8.5.3.8 Análisis de Riesgo Periódico

Servicio de análisis y de mejora continua de la seguridad de la empresa. Este servicio recogerá información de procesos, tecnología, monitoreo y análisis de seguridad con el objetivo de generar tableros de control con la posición de seguridad empresarial. Establecerá tareas de mejora continua de seguridad y permitirá su seguimiento a lo largo del tiempo mediante tableros de control.

El Análisis de Riesgo se alimentará de información del CyberSOC, de análisis de vulnerabilidades, de roadmaps o exploración, entre otros, con el objetivo de generar tableros de control, indicadores de riesgo y recomendaciones e iniciativas. Con el Análisis de Riesgo el contratista establecerá métricas de seguridad para seguimiento y brinda información relevante para atención técnica y la toma de decisiones.

8.5.3.9 Security Rating

Las calificaciones de seguridad serán una medición dinámica, objetiva y basada en datos de la postura de seguridad de San Gabán.

Deberá monitorear y recopilar miles de puntos de datos diariamente a través de métodos comerciales, de código abierto y patentados confiables. Se debe centrar en la recopilación de datos pasiva y no invasiva, que se puede realizar de forma única a escala y bajo demanda. Deberá buscar constantemente nuevas comprobaciones a lo largo del tiempo, lo que significa que actualizarán su algoritmo de calificación para reflejar mejor lo que consideramos la mejor postura de seguridad.

Una vez recopilados o actualizados, todos sus controles se introducirán en un algoritmo de calificación para producir una calificación de seguridad de 950 para todas las propiedades web de una organización con acceso a Internet. Las propiedades web deberán comenzar con una calificación de 950 y se le restarán puntos por cada verificación que no pasan. La cantidad de puntos deducidos se basa en la gravedad y el peso del riesgo subyacente. Para producir la



calificación de seguridad general de San Gabán calcularán un promedio ponderado de todas las puntuaciones de los activos individuales, donde las puntuaciones más bajas reciben la mayor ponderación.

Clasificación de gravedad

- Riesgos críticos. Riesgos o vulnerabilidades que colocan a la empresa en riesgo inmediato de sufrir violaciones de datos.
- Riesgos graves. Riesgos Altos y deben abordarse de inmediato para proteger el negocio.
- Riesgos medios. Riesgos de seguridad que pueden conducir a vulnerabilidades más graves.
- Riesgos bajos. Áreas de mejora para reducir el riesgo y mejorar la seguridad cibernética de las empresas.

Categorización de riesgos

- Deberá mostrar un total de seis categorías en el sistema de evaluación actual.
- Cada categoría estará asociada con varios controles que conllevan pesos/costos fijos.
- Si un sitio web no supera una de esas comprobaciones, perderá puntuación para esa categoría.

8.5.3.10 Análisis forense informático

El análisis forense informático es la agrupación de técnicas de análisis especializadas en las infraestructuras tecnológicas IT y también OT. Estas técnicas nos posibilitan realizar una identificación, análisis y presentación de datos y documentación, que puede permitir evidenciar algún patrón o anomalía que se busca identificar. El análisis forense Informático es, por tanto, un análisis que se realiza una vez se ha detectado la amenaza y ésta se ha materializado.

El Análisis Forense nos permitirá analizar las causas y consecuencias que han producido en los sistemas informáticos de la empresa, averiguar quién ha sido el autor, las causas, la metodología empleada y detectar las debilidades de nuestros sistemas informáticos que han ocasionado el ataque.

El contratista realizará un máximo de 3 análisis forense informático durante la cobertura del contrato.

8.5.3.11 Visibilidad de vulnerabilidades

Se deberá de entregar un reporte trimestral que permita tener la visibilidad de las vulnerabilidades existentes en la red de San Gabán, debiendo dar cobertura a los activos de la red TI como los siguientes:

- Dispositivos de red.
- Equipos con Sistemas operativos (Windows, MacOS y Linux).
- Dispositivos de seguridad.

8.6 OBLIGACIONES DEL CONTRATISTA

El Proveedor es el responsable directo y absoluto de las actividades que realizará, ya sea directamente o a través de su personal, debiendo responder por el servicio brindado.

8.6.1 Niveles de Servicio de CyberSOC

Servicio	SLA	Reportes y Accesos
Monitoreo de salud de la plataforma	Disponibilidad diaria 24x7x365	Detección de casos de uso establecidos. Resumen semanal. Consolidado mensual del servicio.
Monitoreo avanzado tiempo real y correlación de eventos de seguridad	Disponibilidad diaria 24x7x365	Detección de casos de uso establecidos. Resumen semanal. Consolidado mensual del servicio.
Cyber Threat Intelligence (Inteligencia de Ciberseguridad)	Disponibilidad diaria 24x7x365	Informe de Inteligencia periódico.
Threat Hunting	Disponibilidad diaria 24x7x365	Atención de casos de seguridad avanzados
Alerta Temprana	Disponibilidad diaria 24x7x365	Envío de alertas de acuerdo con la matriz de comunicación.
Portal de Supervisión	Disponibilidad diaria 24x7x365	Acceso al Dashboard personalizado de reporte.



Advanced Security Incident Response (Respuesta Avanzada a Incidentes)					
Preparación	Tiempo promedio de detección e inicio del análisis	Tiempo promedio de contención	Tiempo promedio de reparación	Tiempo promedio de resolución	Análisis de repercusiones
Permanente	< 30 minutos	< 45 minutos	< 3 horas	< 6 horas	Dentro de las 48 horas de resuelto el incidente.
Tiempos de Atención Off-Site					
Disponibilidad 24 x 7 x 365 2 horas de atención en Lima Metropolitana					
Dimensionamiento		Capacidad de SOC a ser contratada			
Eventos por segundo (EPS)		500			
Casos de uso		10			

8.6.2 Niveles del servicio del Servicio de Operación de la solución de Ciberseguridad

Servicio	SLA	Entregables
Gestor de Servicio	Supervisión cotidiana. Asistencia a comités de seguridad mensuales.	
Operador del servicio	Operación cotidiana a cargo del Gestor de Servicio en horario de oficina (24x7).	Informe de actividad técnica semanal. Informe de servicio mensual.
Cambios, Configuraciones y Maniobras	Número de solicitudes: Ilimitado Horario: 24x7 SLA: P2, P3 o P4.	Solicitud/resolución individual.
Soporte técnico	Número de solicitudes: Ilimitado Horario: 24x7 SLA: P1, P2, P3 o P4.	Solicitud/resolución individual.
Copias de respaldo	Periodicidad: Semanal. SLA: 99.8% de cumplimiento	Informe técnico.
Actualizaciones y mejoras	Periodicidad: De acuerdo con el plan de mejoras. SLA: 99.8% de cumplimiento	Informe técnico.

Niveles de criticidad aceptados	
Son categorizaciones estándar para labor del área de soporte técnico. Cada vez que un caso o incidente sea reportado, el ingeniero de Bafing asignará un nivel de criticidad de acuerdo con la información proporcionada.	
Nivel “crítico” o “de emergencia”	<ul style="list-style-type: none"> Situación: El negocio o servicios críticos del cliente han sido afectados Prioridad asignada: “P1”
Nivel “alto”	<ul style="list-style-type: none"> Situación: Servicios no críticos han sido afectados. Problema ha sido controlado temporalmente por el cliente. Probabilidad que se afecte sistemas críticos del negocio en el corto plazo. Prioridad asignada: “P2”
Nivel “medio” o “moderado”	<ul style="list-style-type: none"> Situación: Se necesita más información para determinar posible impacto. Existen incongruencias en la solución. Prioridad asignada: “P3”
Nivel “bajo” o “rutina”	<ul style="list-style-type: none"> Situación: Actividades de Adición, Modificación, Eliminación, Ajuste. Labores para efectuar bajo programación. Prioridad asignada: “P4”
Nivel “informativo”	<ul style="list-style-type: none"> Se incluyen también actividades de intercambio de información donde no se requiere ninguna acción. Prioridad asignada: “P5”

8.6.3 Tiempos de Atención para Cambios, Configuraciones, Maniobras y Soporte

P5	P4	P3	P2	P1
Nivel Informativo	Nivel bajo o rutina	Nivel medio/moderado	Nivel alto	Nivel crítico o de emergencia
TIEMPO DE EJECUCIÓN PARA CAMBIOS Y CONFIGURACIONES				
48:00:00	24:00:00	24:00:00	12:00:00	4:00:00
TIEMPO DE RESOLUCIÓN ESPERADA PARA INCIDENTES				
24:00:00	12:00:00	6:00:00	4:00:00	2:00:00
Los tiempos SLA se contabilizan en horas desde el ingreso de la solicitud. Algunas labores de cambios y configuraciones complejas requieren acciones de planificación, validación o pruebas complementarias y que incluso pueden depender de proveedores terceros.				

8.6.4 Canales de Atención Disponibles

- **Telefónico.** - Se brindará a través de medios de telefonía fija o móvil, se debe entregar una cartilla trimestral de atención de contacto.
- **E-mail y Chat.** Se brindará a través de comunicación electrónica como e-mail y chat (mensajería instantánea). Para el caso de e-mail, se recibirán nuestras 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, el cual es un método rápido y seguro. La conexión remota puede ser establecida mediante conexión VPN o conexión a escritorio remoto mediante software cliente certificado.

8.6.5 Membresías y acreditaciones del CyberSOC

- Debe ser miembro de la asociación ICSPA (*International Cyber Security Protection Alliance*) con el objetivo de canalizar experiencia y asistencia directamente para ayudar a las unidades de delitos cibernéticos de aplicación de la ley en los mercados nacionales e internacionales.
- Requerimiento opcional, ser miembro de la asociación FIRST (*Forum of Incident Response and Security Teams, Inc.*) con el objetivo de formar una alianza de equipos de investigación y respuesta global de seguridad que cumplan con los criterios de elección y de auditoría de FIRST.
- Contar con certificación ISO 27001 vigente.
- Open CSIRT - SIMv3-2021 o más actual (nivel de madurez)
- SOC-CMM v2.x (nivel de madurez)

8.7 INFORMES UNIFICADOS

De manera periódica, se deberán presentar los siguientes tipos de informes, de manera digital, por correo electrónico a ccastro@sangaban.com.pe, llizares@sangaban.com.pe, y mgordillo@sangaban.com.pe :

- a. Informe mensual del servicio, requerido para el pago de las facturas mensuales
- b. Informe mensual del NOC y del SOC.
- c. Informe de incidentes (a las 24 horas de la ocurrencia) y su mitigación, según el caso.
- d. Informes de salud del servicio.
- e. Informes para comunicar al CSIRT (formato estándar).

8.8 PERSONAL DEL CONTRATISTA

8.8.1 Personal No Clave

Un (1) Gestor del servicio: Debe ser un Ingeniero en Computación, o Computación y Sistemas, o Informática, o Sistemas, o Sistemas y Cómputo. Contar con certificaciones técnicas vigentes en plataformas de ciberseguridad de por lo menos tres (03) fabricantes. Contar con una Experiencia mínima de cinco (05) años en la gestión de plataformas de ciberseguridad.

Un (1) Operador del servicio como mínimo: Debe ser Bachiller o Ingeniero en Computación, o Computación y Sistemas, o Informática, o Sistemas, o Sistemas y Cómputo. Contar con certificaciones técnicas vigentes en plataformas de ciberseguridad de por lo menos tres (03) fabricantes. Tener una experiencia mínima de tres (03) años en la gestión de plataformas de ciberseguridad.

Tres (3) personas para el equipo de NOC (Command Center): Los miembros del equipo deben ser nivel Técnico o Bachiller o Ingeniero en Computación, o Computación y Sistemas, o Informática, o Sistemas, o Sistemas y Cómputo. Contar con certificaciones técnicas vigentes en plataformas de ciberseguridad de por lo menos dos (02) fabricantes. Tener una experiencia mínima de tres (03) años en la gestión de plataformas de ciberseguridad.

Las evidencias del personal **No Clave**, deben presentarse para la etapa de perfeccionamiento del contrato, con CV firmado, el título o documento que acredite nivel de técnico o bachiller o ingeniero; las certificaciones mediante constancias, certificados u otros documentos según corresponda; la experiencia señalada para cada caso mediante certificados y/o constancias de trabajo, contratos u/o cualquier documento que acredite la experiencia señalada.



8.9 OBLIGACIONES DE SAN GABÁN S.A.

San Gabán proveerá lo siguiente para la implementación del servicio

- b) **Comunicaciones.** Enlace VPN permanente desde el Data Center del CyberSOC hacia los sistemas de recolección de EGE San Gabán.
- c) **Servidor de recolección.** Sistema virtual donde se instalará un sistema de recolección para el SIEM que permitirá la transmisión de eventos hacia el Data Center del CyberSOC del contratista.
- d) **Servidor de recolección (físico o virtual)**
 - VMware ESXi 6.5 o superior.
 - 4 vCPU Cores.
 - 16 GB RAM.
 - 500 GB - Disco.
- e) **Servidor de monitoreo.** Sistema virtual donde se instalará un sistema de monitoreo del estado de salud de las plataformas de seguridad hacia el Data Center del CyberSOC del contratista.
- f) **Servidor de monitoreo (físico o virtual)**
 - Windows Server 2019.
 - 4 vCPU Cores.
 - 8 GB RAM.
 - 250 GB – Disco.

9. SEGUROS

No aplica para la presente contratación.

10. MEDIDAS DE SEGURIDAD EN LA PRESTACIÓN DEL SERVICIO

No aplica para la presente contratación.

11. REQUISITOS DE CALIFICACIÓN

C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a Tres Cientos Mil con 00/100 Soles (S/300,000.00), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de Cincuenta Mil con 00/100 soles (S/50,000.00), 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. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.</p> <p>Se consideran servicios similares a los siguientes: servicio de seguridad SOC, servicio de ciberseguridad, servicio de seguridad perimetral, servicio de seguridad de la red interna y perimetral.</p> <p><u>Acreditación:</u></p> <p>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de 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.</p>

⁹ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado:**



correspondientes a un máximo de veinte (20) contrataciones.

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

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

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

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

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

Si el postor acredita experiencia de 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 N° 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*

“... 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 que 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 debería reconocerse la validez de la experiencia”.



Contrataciones del Estado”.

12. PLAZO DE EJECUCIÓN

El plazo de ejecución es de 731 (setecientos treinta y un) días calendario, el mismo que se computa desde la suscripción del **Acta de Conformidad de Inicio del Servicio**.

El plazo para la implementación del servicio es de máximo 30 (treinta) días calendario, el mismo que se computa desde el día siguiente de la firma del contrato y culmina con la suscripción del **Acta de Conformidad de Inicio del Servicio**.

13. LUGAR DE PRESTACIÓN DEL SERVICIO

El lugar de prestación de la contratación se realizará en la sede administrativa de la empresa sito en Av. Floral 245, ciudad, distrito y departamento de Puno. El servicio podrá ser implementado virtualmente utilizando accesos virtuales (VPN).

14. REAJUSTES

No aplica para esta contratación.

15. PENALIDAD POR MORA

Si EL CONTRATISTA incurre en retraso injustificado en la ejecución de las prestaciones objeto de la contratación, LA ENTIDAD le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo con 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.

- Tanto el monto vigente como el plazo vigente se refieren, según corresponda, al total de la contratación, o en caso de ejecución periódica o continua, a la prestación parcial que fuera materia del retraso.
- Se considera justificado el retraso cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable.
- Esta calificación del retraso como justificado no da lugar a pago de gastos generales de ningún tipo.

16. OTRAS PENALIDADES

No aplica para esta contratación.

17. CONFIDENCIALIDAD

La confidencialidad y reserva absoluta en el manejo de información y documentación a la que se tenga acceso relacionada con la prestación, pudiendo quedar expresamente prohibido revelar dicha información a terceros. El CONTRATISTA, debe dar cumplimiento a todas las políticas y estándares definidos por SAN GABÁN S.A., en materia de seguridad de la información.

Esta 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 mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos, diagnósticos, documentos, cuadros comparativos y demás datos compilados o recibidos por el CONTRATISTA.

18. CONSIDERACIONES GENERALES A LOS PRODUCTOS

Los derechos intelectuales de los productos y documentos elaborados por el CONTRATISTA que resulte seleccionado son propiedad de SAN GABÁN S.A., así como toda aquella información interna de la institución a la que tenga acceso para la ejecución del servicio.



La difusión, publicación o utilización de dicha propiedad intelectual deberá ser previamente autorizada por SAN GABÁN S.A.

19. RESPONSABILIDAD DEL CONTRATISTA

El contratista es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofertado por un plazo no menor **de 1 año**, contado a partir de la conformidad otorgada por la Entidad.

20. OBLIGACIÓN ANTICORRUPCIÓN Y ANTISOBORNO

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, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación con la contratación.

Asimismo, el contratista se obliga a conducirse en todo momento, durante la ejecución de la contratación, 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.

Además, el contratista debe 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 los párrafos anteriores, durante la ejecución contractual, da el derecho a SAN GABÁN S.A. a resolver automáticamente y de pleno derecho la contratación, bastando para tal efecto que se remita una comunicación informando que se ha producido dicha resolución, sin perjuicio de las acciones civiles, penales y administrativas que SAN GABÁN S.A. pueda accionar.

21. PRESTACIONES ACCESORIAS

No aplica para esta contratación.

22. CONFORMIDAD

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 la Oficina de Tecnologías de la Información y Comunicaciones.

23. FORMA Y CONDICIONES DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista considerará el siguiente detalle:

Descripción	Requisitos
Primer pago: (VL) Valor del Licenciamiento	1. Incluye la instalación, configuración, despliegue, capacitación y todo aspecto con conlleve a la puesta en operación del producto o suite antimalware. Se emitirá un Acta de Recepción e Inicio del Servicio. 2. La conformidad de la Oficina de TIC.
Valorizaciones mensuales: (VS) Valor del servicio gestionado (12 pagos al final de cada mes) y 1 día antes del último día hábil del mes.	1, Previa presentación del informe mensual de la seguridad gestionada, los reportes de incidentes con los tiempos de atención reales por cada ticket generado, y con las conclusiones y recomendaciones; tanto del NOC y del SOC. 2. La conformidad de la Oficina de TIC.

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

- Informe del funcionario responsable del Oficina de Tecnologías de la Información y Comunicaciones emitiendo la conformidad de la prestación efectuada.
- Comprobante de pago (**FACTURA ELECTRONICA y su archivo de extensión .xml**).
- **Carta o documento donde el contratista señala el número de cuenta corriente, CCI y nombre de la**



entidad bancaria, para el trámite pago.

- Informe mensual unificado.

Dicha documentación se debe presentar en Mesa de Partes Virtual San Gabán S.A. mesadepartes@sangaban.com.pe con copia a facturalogistica@sangaban.com.pe, si es físicamente será en la Sede Administrativa sito en Av. Floral 245, ciudad, distrito y departamento de Puno.

La Entidad debe pagar las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días calendario siguientes a la conformidad, siempre que se haya verificado el cumplimiento de las condiciones establecidas en los TERMINOS DE REFERENCIA y orden de servicio.



3.2. REQUISITOS DE CALIFICACIÓN

C	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u> El postor debe acreditar un monto facturado acumulado equivalente a S/300,000 (Tres Cientos Mil y 00/100 Soles), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de cincuenta mil con 00/100 soles (S/ 50,000.00), 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. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.</p> <p>Se consideran servicios similares a los siguientes: servicio de seguridad SOC, servicio de ciberseguridad, servicio de seguridad perimetral, servicio de seguridad de la red interna y perimetral.</p> <p><u>Acreditación:</u> 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 pago¹⁰, correspondientes a un máximo de veinte (20) contrataciones.</p> <p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.</p> <p>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.</p> <p>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.</p> <p>Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva “Participación de Proveedores en Consorcio en las Contrataciones del Estado”, debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de</p>

¹⁰ 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 que 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 debería 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 N° 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".*



**CAPÍTULO IV
FACTORES DE EVALUACIÓN**

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



CAPÍTULO V PROFORMA DEL CONTRATO

Conste por el presente documento, la contratación del servicio de [CONSIGNAR LA DENOMINACIÓN DE LA CONVOCATORIA], que celebra de una parte [CONSIGNAR EL NOMBRE DE LA ENTIDAD], en adelante LA ENTIDAD, con RUC N° [.....], con domicilio legal en [.....], representada por [.....], identificado con DNI N° [.....], y de otra parte [.....], con RUC N° [.....], con domicilio legal en [.....], inscrita en la Ficha N° [.....] Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], debidamente representado por su Representante Legal, [.....], con DNI N° [.....], según poder inscrito en la Ficha N° [.....], Asiento N° [.....] del Registro de Personas Jurídicas de la ciudad de [.....], a quien en adelante se le denominará EL CONTRATISTA en los términos y condiciones siguientes:

CLÁUSULA PRIMERA: ANTECEDENTES

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

CLÁUSULA SEGUNDA: OBJETO

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

CLÁUSULA TERCERA: MONTO CONTRACTUAL

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

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

CLÁUSULA CUARTA: DEL PAGO¹¹

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

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

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

¹¹ En cada caso concreto, dependiendo de la naturaleza del contrato, podrá adicionarse la información que resulte pertinente a efectos de generar el pago.



[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 en el literal a) del numeral 155.1 del artículo 155 del Reglamento de la Ley de Contrataciones del Estado.

Preferentemente la(s) garantía(s) será(n) renovada(s) con ocho (8) días antes de su vencimiento.

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 cumpliera a cabalidad con la subsanación, LA ENTIDAD puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar.

Este procedimiento no resulta aplicable cuando los 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 [CONSIGNAR TIEMPO EN AÑOS, NO MENOR DE UN (1) AÑO] año(s) 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.

Cuando se llegue a cubrir el monto máximo de la penalidad por mora, 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: RESPONSABLE DEL CONTRATO

SAN GABÁN S.A., designa como Administrador del Contrato, al funcionario que se encuentra desempeñando funciones en el puesto de de la Gerencia de de la Empresa de Generación Eléctrica San Gabán S.A., con el fin de controlar el cabal cumplimiento de las condiciones y obligaciones pactadas en el presente contrato, Bases Administrativas, Términos de Referencia y Propuesta Técnica - Económica.

El Administrador del Contrato, será responsable de verificar y exigir la correcta prestación objeto del presente contrato y de asegurar el fiel cumplimiento de las condiciones estipuladas y las obligaciones de EL CONTRATISTA; en consecuencia, de manera enunciativa y no limitativa, está facultado para lo siguiente:

....1 Podrá solicitar la información que considere pertinente a EL CONTRATISTA, sobre la prestación materia del presente contrato. Asimismo, recibirá toda la información que remita EL CONTRATISTA.

....2 No podrá relevar a EL CONTRATISTA, de ninguna de las obligaciones establecidas en el presente contrato.

....3 Suscribirá el Acta de Conformidad Final por la prestación materia del presente contrato.

CLÁUSULA DÉCIMA OCTAVA: SOLUCIÓN DE CONTROVERSIAS¹²

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 el derecho a iniciar el arbitraje administrativo 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 de tipo institucional administrado.

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° Reglamento de la Ley de Contrataciones del Estado, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un acuerdo.

¹² 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).



entre ambas o se llegue a un acuerdo parcial. Las controversias sobre la nulidad del contrato sólo pueden ser sometidas a arbitraje.

Todos los conflictos que se deriven de la ejecución e interpretación del presente contrato, incluidos lo que se refieren a su nulidad e invalidez, serán resueltos mediante arbitraje, de conformidad con los Reglamentos Arbitrales del Centro de Arbitraje de la Cámara de Comercio y la Producción de Puno “CA-CCP/P”, a cuyas normas, administración y decisión se someten las partes en forma incondicional.

El Arbitraje será resuelto por un Tribunal Arbitral, compuesto por tres árbitros (artículo 230° del Reglamento de la Ley de Contrataciones del Estado); cada una de las partes nombrará un árbitro y el tercero será designado por los árbitros ya elegidos. Ante la rebeldía de una de las partes en cumplir con dicha designación, ésta será efectuada de acuerdo a lo reglamentado por el Centro de Arbitraje de la Cámara de Comercio y la Producción de Puno “CA-CCP/P”.

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

CLÁUSULA DÉCIMA NOVENA: FACULTAD DE ELEVAR A ESCRITURA PÚBLICA

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

CLÁUSULA VIGÉSIMA: DOMICILIO PARA EFECTOS DE LA EJECUCIÓN CONTRACTUAL

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

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

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

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

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

“LA ENTIDAD”

“EL CONTRATISTA”

Importante

Este documento puede firmarse digitalmente si ambas partes cuentan con firma digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales¹³.

¹³ Para mayor información sobre la normativa de firmas y certificados digitales ingresar <https://www.indecopi.gob.pe/web/firmas-digitales/firmar-y-certificados-digitales>



ANEXOS



ANEXO Nº 1**DECLARACIÓN JURADA DE DATOS DEL POSTOR**

Señores

COMITÉ DE SELECCIÓN**ADJUDICACION SIMPLIFICADA Nº AS-043-2023-SAN GABAN S.A. Primera Convocatoria**

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] Nº [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 ¹⁴		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 servicios¹⁵

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.

¹⁴ Esta información será verificada por la Entidad en la página web del Ministerio de Trabajo y Promoción del Empleo en la sección consulta de empresas acreditadas en el REMYPE en el link <http://www2.trabajo.gob.pe/servicios-en-linea-2-2/> y se tendrá en 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. Asimismo, dicha información se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento.

¹⁵ Cuando el monto del valor estimado del procedimiento o del ítem no supere los doscientos mil Soles (S/ 200,000.00), en caso se haya optado por perfeccionar el contrato con una orden de servicios.



Importante

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

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

COMITÉ DE SELECCIÓN

ADJUDICACION SIMPLIFICADA N° AS-043-2023-SAN GABAN S.A. Primera Convocatoria

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 ¹⁶	Sí		No	
Correo electrónico :				

Datos del consorciado 2				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁷	Sí		No	
Correo electrónico :				

Datos del consorciado ...				
Nombre, Denominación o Razón Social :				
Domicilio Legal :				
RUC :	Teléfono(s) :			
MYPE ¹⁸	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.

¹⁶ 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. Asimismo, dicha información se tendrá en cuenta en caso de empate, conforme a lo previsto en el artículo 91 del Reglamento. Para dichos efectos, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

¹⁷ Ibidem.

¹⁸ Ibidem.



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 servicios¹⁹

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.

¹⁹ Cuando el monto del valor estimado del procedimiento o del ítem no supere los doscientos mil Soles (S/ 200,000.00), en caso se haya optado por perfeccionar el contrato con una orden de servicios.



ANEXO Nº 2

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

Señores

COMITÉ DE SELECCIÓN

ADJUDICACION SIMPLIFICADA Nº AS-043-2023-SAN GABAN S.A. Primera Convocatoria

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 Nº 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

ADJUDICACION SIMPLIFICADA Nº AS-043-2023-SAN GABAN S.A. Primera Convocatoria

Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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



ANEXO Nº 4

DECLARACIÓN JURADA DE PLAZO DE PRESTACIÓN DEL SERVICIO

Señores

COMITÉ DE SELECCIÓN

ADJUDICACION SIMPLIFICADA Nº AS-043-2023-SAN GABAN S.A. Primera Convocatoria

Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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



ANEXO N° 5

PROMESA DE CONSORCIO

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

Señores

COMITÉ DE SELECCIÓN

ADJUDICACION SIMPLIFICADA N° AS-043-2023-SAN GABAN S.A. Primera Convocatoria

Presente.-

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

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

a) Integrantes del consorcio

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

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

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

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

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

1. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 1] [%]²⁰

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE [NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2] [%]²¹

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

TOTAL OBLIGACIONES



[CONSIGNAR CIUDAD Y FECHA]

²⁰ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

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

²² Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

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

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

Importante

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



ANEXO N° 6**PRECIO DE LA OFERTA**

Señores

COMITÉ DE SELECCIÓN**ADJUDICACION SIMPLIFICADA N° AS-043-2023-SAN GABAN S.A. Primera Convocatoria**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 CIBERSEGURIDAD IT CON SEGURIDAD ADMINISTRADA	
TOTAL S/	

El precio de la oferta 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

- El postor debe consignar el precio total de la oferta, sin perjuicio que, de resultar favorecido con la buena pro, presente el detalle de precios unitarios para el perfeccionamiento del contrato.*
- En caso que el postor reduzca su oferta, según lo previsto en el artículo 68 del Reglamento, debe presentar nuevamente este Anexo.*
- El postor que goce de alguna exoneración legal, debe indicar que su oferta no incluye el tributo materia de la exoneración, debiendo incluir el siguiente texto:*

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



**ANEXO Nº 8
EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD**

Señores
COMITÉ DE SELECCIÓN
ADJUDICACION SIMPLIFICADA Nº AS-043-2023-SAN GABAN S.A. Primera Convocatoria
Presente.-

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

Nº	CLIENTE	OBJETO DEL CONTRATO	Nº CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ²³	FECHA DE LA CONFORMIDAD DE SER EL CASO ²⁴	EXPERIENCIA PROVENIENTE ²⁵ DE:	MONEDA	IMPORTE ²⁶	TIPO DE CAMBIO VENTA ²⁷	MONTO FACTURADO ACUMULADO ²⁸
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
...										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

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

²³ 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.

²⁴ 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.

²⁵ 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 Nº 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 Nº 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".

²⁶ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

²⁷ 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.

²⁸ Consignar en la moneda establecida en las bases.



ANEXO Nº 9

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

Señores

COMITÉ DE SELECCIÓN

ADJUDICACION SIMPLIFICADA Nº AS-043-2023-SAN GABAN S.A. Primera Convocatoria

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 Nº 11

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

Señores

COMITÉ DE SELECCIÓN

ADJUDICACION SIMPLIFICADA Nº AS-043-2023-SAN GABAN S.A. Primera Convocatoria

Presente.-

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

[CONSIGNAR CIUDAD Y FECHA]

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

Importante

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



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

ADJUDICACION SIMPLIFICADA N° AS-043-2023-SAN GABAN S.A. Primera Convocatoria

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.

