

SIMBOLOGÍA UTILIZADA:

Nº	Símbolo	Descripción
1	[ABC]	Es una indicación que debe ser completada o eliminada por la entidad contratante durante la elaboración de las bases conforme a las instrucciones brindadas.
2	<u>[ABC]</u>	Es una indicación o información que debe ser completada por la entidad contratante con posterioridad al otorgamiento de la buena pro para el caso específico de la elaboración de la PROFORMA DEL CONTRATO; o por los proveedores, al completar los ANEXOS de la oferta.
3	<div>Advertencia</div> <div>• Abc</div>	Se refiere a advertencias a tener en cuenta por los evaluadores y los proveedores. No deben ser eliminadas.
4	<div>Importante para la entidad contratante</div> <div>• Xyz</div>	Se refiere a consideraciones importantes a tener en cuenta por los evaluadores y deben ser eliminadas una vez culminada la elaboración de las bases.

CARACTERÍSTICAS DEL DOCUMENTO:

Las bases deben ser elaboradas en formato WORD, y deben tener las características del presente documento. De existir algún cambio en el formato como márgenes, fuente, tamaño de letra, entre otros, no acarrea su nulidad, salvo que por el tipo o tamaño de letra impida la lectura por parte de los proveedores.

INSTRUCCIÓN DE USO:

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

BASES ESTÁNDAR CONCURSO PÚBLICO DE SERVICIOS

**CONCURSO PÚBLICO DE SERVICIOS N°
007.2025.CORPAC S.A. –
PRIMERA CONVOCATORIA**

**CONTRATACIÓN DE SERVICIOS EN GENERAL
SERVICIO DE MONITOREO Y ALERTA DE SEGURIDAD -
CYBERSOC**

SECCIÓN GENERAL

DISPOSICIONES COMUNES DEL CONCURSO PÚBLICO DE SERVICIOS

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

CAPÍTULO I

ASPECTOS GENERALES

1.1. REFERENCIAS

Cuando en el presente documento se mencione la palabra Ley, se entiende que se está haciendo referencia a la Ley N° 32069, Ley General de Contrataciones Públicas, y cuando se mencione la palabra Reglamento, se entiende que se está haciendo referencia al Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF. Las referidas normas incluyen sus respectivas modificaciones, de ser el caso.

1.2. ALCANCE

La presente base estándar correspondiente al procedimiento de selección de Concurso Público de Servicios se utiliza por la entidad contratante para la contratación de servicios en general, según la cuantía establecida en la Ley de Presupuesto del Sector Público para el Año Fiscal correspondiente.

CAPÍTULO II DESARROLLO DEL PROCEDIMIENTO DE SELECCIÓN

2.1 ETAPAS DEL CONCURSO PÚBLICO DE SERVICIOS

Las etapas del procedimiento de selección de Concurso Público de Servicios son las siguientes:

ETAPA	CARACTERÍSTICAS	BASE LEGAL
a) Convocatoria	Se realiza a través del SEACE de la Pladicop en la fecha señalada en el cronograma.	Artículos 63 y 64 del Reglamento.
b) Registro de participantes	Aplica lista abierta, por lo que cualquier proveedor puede registrarse como participante en el procedimiento de selección.	Artículos 65 y 94 del Reglamento.
c) Cuestionamientos a las bases (consultas, observaciones e integración)	<ol style="list-style-type: none"> 1. La presentación de consultas y observaciones se realiza en un plazo no menor a siete días hábiles contabilizados desde el día siguiente de la convocatoria. 2. La absolución de los referidos cuestionamientos y la publicación de las bases integradas se realiza en la fecha prevista en el cronograma del procedimiento de selección. 3. El pliego de absolución de consultas y observaciones y las bases integradas pueden ser elevadas al OECE en un plazo de tres días hábiles siguientes de publicados, conforme las condiciones indicadas en la directiva respectiva del OECE. <u>La entidad contratante puede omitir la posibilidad de elevar al OECE el pliego de absolución de consultas y observaciones o las bases integradas en caso haya utilizado la herramienta de difusión del requerimiento en la interacción con el mercado.</u> 	Artículos 51, 66, 67 y 94 del Reglamento.
d) Evaluación de ofertas técnicas y económicas	<ol style="list-style-type: none"> 1. La presentación de ofertas se realiza a través del SEACE de la Pladicop en un plazo no menor <u>de siete días hábiles</u> contabilizados desde la publicación de la integración de bases o el pronunciamiento con la integración definitiva de bases por parte del OECE. 2. Las ofertas son presentadas por los participantes desde las 00:01 horas hasta las 23:59 horas del día (hora peruana), según el cronograma del procedimiento de selección; adjuntando el archivo digitalizado que contenga los documentos que conforman la oferta de acuerdo con lo requerido en las bases. 3. La evaluación de ofertas es <u>SIN PRECALIFICACIÓN</u> y consiste en: <ol style="list-style-type: none"> a. Admisión de las ofertas: Los evaluadores revisan que la oferta contenga los 	Artículos 72, 73, 74, 75 y 78 del Reglamento.

	<p>documentos señalados en el Capítulo II de la Sección Específica de las bases, caso contrario la oferta se considera no admitida.</p> <p>b. Revisión de los requisitos de calificación: Los evaluadores califican a los postores verificando que cumplan con los requisitos de calificación detallados en el Capítulo III de la Sección Específica de las bases. Caso contrario la oferta se considera descalificada.</p> <p>c. Evaluación de ofertas técnicas: Los evaluadores aplican los factores de evaluación previstos en el Capítulo IV de la Sección Específica de las bases a las ofertas que cumplen los requisitos de calificación. En la sección específica se prevé un puntaje mínimo en la evaluación técnica para proceder a la evaluación económica de la oferta.</p> <p>d. Evaluación de ofertas económicas: La evaluación de la oferta económica es <u>posterior a la evaluación de la oferta técnica y solo respecto de aquellos proveedores que hubieran obtenido un puntaje mínimo en dicha evaluación.</u></p> <p>4. Todos los actos se realizan a través del SEACE de la Pladicip, incluyendo la subsanación de ofertas.</p>	
e) Otorgamiento de la buena pro	<p>1. Definida la oferta ganadora, los evaluadores otorgan la buena pro mediante su publicación en el SEACE de la Pladicip, incluyendo los documentos que sustenten los resultados de la admisión, calificación, evaluación y el otorgamiento de la buena pro.</p> <p>2. En caso de haber sorteo por desempate, éste se realiza a través del SEACE de la Pladicip.</p> <p>3. En caso se hayan presentado dos o más ofertas, el consentimiento de la buena pro es publicado a través del SEACE de la Pladicip al día siguiente de vencido el plazo correspondiente para interponer recurso de apelación, sin que los postores hayan ejercido el derecho de interponer dicho recurso.</p> <p>En caso de que se haya presentado una sola oferta, el consentimiento de la buena pro se produce el mismo día de la notificación de su otorgamiento.</p>	Artículos 80, 81, 82, 83 y 84 del Reglamento.

2.2 EVALUACIÓN DE OFERTAS ECONÓMICAS QUE SUPEREN LA CUANTÍA DE LA CONTRATACIÓN

- 2.2.1.** En caso la oferta económica del postor que obtiene el mejor puntaje total supere la cuantía de la contratación, se siguen los siguientes pasos:

- i. La DEC gestiona la solicitud de la ampliación de la certificación o previsión presupuestal correspondiente. De otorgarse la ampliación, se procede a adjudicar la buena pro.
- ii. De no contar con la ampliación de la certificación o previsión presupuestal, los evaluadores negocian con el postor con el mejor puntaje total la reducción del monto o la reducción de las prestaciones o condiciones del requerimiento, conforme al numeral 132.1 del artículo 132 del Reglamento.
- iii. En caso el postor con el mejor puntaje total no acepte, se procede a negociar con los siguientes postores en orden de prelación. Si el postor que procede en el orden de prelación ofertó un monto por debajo de la cuantía de la contratación, se le adjudica la buena pro.
- iv. En caso el postor que obtuvo el mejor puntaje total reduzca su oferta económica pero la reducción no se encuentre dentro de la cuantía de la contratación, se solicita la ampliación de la certificación de crédito presupuestario y/o previsión presupuestal correspondiente. En caso se otorgue la ampliación, se adjudica la buena pro. Caso contrario, se puede optar por negociar con los siguientes postores en el orden de prelación o declarar desierto el procedimiento de selección.
- v. Las decisiones adoptadas por los evaluadores en la negociación constan en actas que se publican en el SEACE de la Pladipoc y se sustentan en el principio de valor por dinero, priorizando el cumplimiento de la finalidad pública de la contratación.

2.3 CONSIDERACIONES PARA TODOS LOS PROVEEDORES:

- 2.3.1 Para registrarse como participante en un procedimiento de selección convocado por una entidad contratante, es necesario que los proveedores cuenten con inscripción vigente ante el Registro Nacional de Proveedores (RNP) que administra el Organismo Especializado para las Contrataciones Públicas Eficientes (OECE). Para obtener mayor información, se puede ingresar a la siguiente dirección electrónica: www.rnp.gob.pe.
- 2.3.2 Los proveedores que deseen registrar su participación deben ingresar al SEACE de la Pladipoc utilizando su certificado (usuario y contraseña).
- 2.3.3 No pueden formularse consultas ni observaciones respecto del contenido de una ficha de homologación aprobada, aun cuando el requerimiento haya sido homologado parcialmente respecto a las características técnicas, requisitos de calificación y/o condiciones de ejecución. Las consultas y observaciones que se formulen sobre el particular se tienen como no presentadas.
- 2.3.4 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 Digitales). No se acepta insertar la imagen de una firma. Las ofertas se presentan foliadas en todas sus hojas. El postor, el representante legal, apoderado o mandatario designado se hace responsable de la totalidad de los documentos que se incluyen en la oferta. El postor es responsable de verificar, antes de su envío, que el archivo pueda ser descargado y su contenido sea legible.
- 2.3.5 En el caso que, al registrarse como participante, el proveedor presente una declaración jurada de desafectación del impedimento debido a parentesco establecido en el inciso 2 del numeral 30.1 del artículo 30 de la Ley, se debe incluir como requisito adicional de admisión de su oferta la acreditación documental de su condición de desafectación, conforme a lo señalado en el numeral 39.4 del artículo 39 del Reglamento.

2.4 CONSIDERACIONES ADICIONALES PARA LOS CONSORCIOS:

- 2.4.1 En el caso de consorcios, basta que uno de sus integrantes se haya registrado como participante en el procedimiento de selección, para lo cual dicho integrante debe contar con inscripción vigente en el RNP como proveedor de servicios. Los demás integrantes del consorcio deben contar con inscripción vigente en el RNP en las demás etapas del procedimiento de selección. No se considera consorcio a la asociación de personas de duración ilimitada o indefinida que, denominándose consorcios, han sido constituidas como personas jurídicas en los Registros Públicos.

- 2.4.2 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. Tratándose de un procedimiento por relación de ítems, los integrantes del consorcio pueden participar en ítems distintos al que se presentaron en consorcio, sea en forma individual o en consorcio.
- 2.4.3 Como parte de los documentos de su oferta el consorcio debe presentar la promesa de consorcio con firmas digitales de todos sus integrantes o, en su defecto, firmas legalizadas, de ser el caso, en la que se consigne lo siguiente:
- a) La identificación de los integrantes del consorcio. Se debe precisar el nombre completo o la denominación o razón social de los integrantes del consorcio, según corresponda.
 - b) La designación del representante común del consorcio.
 - c) El domicilio común del consorcio.
 - d) El correo electrónico común del consorcio, al cual se dirigirán todas las comunicaciones remitidas por la entidad contratante al consorcio durante el proceso de contratación, siendo éste el único válido para todos los efectos.
 - e) Las obligaciones que correspondan a cada uno de los integrantes del consorcio.
 - f) El porcentaje del total de las obligaciones de cada uno de los integrantes, respecto del objeto del contrato. Dicho porcentaje debe ser expresado en número entero, sin decimales.
- 2.4.4 La información contenida en los literales a), e) y f) precedentes no puede ser modificada con ocasión de la suscripción del contrato de consorcio, ni durante la etapa de ejecución contractual. En tal sentido, no cabe variación alguna en la conformación del consorcio, por lo que no es posible que se incorpore, sustituya o separe a un integrante.
- 2.4.5 El representante común tiene facultades para actuar en nombre y representación del consorcio en todos los actos referidos al procedimiento de selección, suscripción y ejecución del contrato, con poderes suficientes para ejercitar los derechos y cumplir las obligaciones que se deriven de su calidad de postor y de contratista hasta la conformidad o liquidación del contrato, según corresponda. El representante común no debe encontrarse impedido, inhabilitado ni suspendido para contratar con el Estado. Para cambiar al representante común, todos los integrantes del consorcio deben firmar (mediante firmas legalizadas o firmas digitales) el documento en el que conste el acuerdo, el cual surte efectos cuando es notificado a la entidad contratante.
- 2.4.6 En el caso de consorcios las declaraciones juradas, formatos o formularios previstos en las bases que conforman la oferta deben estar debidamente firmados por el representante común o por todos los integrantes del consorcio, según corresponda (firma manuscrita o digital, según la Ley N° 27269, Ley de Firmas y Certificados Digitales). En el caso de los documentos que deban suscribir todos los integrantes del consorcio, la firma es seguida de la razón social o denominación de cada uno de ellos. Lo mismo aplica en caso deban ser suscritos en forma independiente por cada integrante del consorcio, de acuerdo con lo establecido en los documentos del procedimiento de selección. En el caso de un consorcio integrado por una persona natural, bastará que la persona natural indique debajo de su firma sus nombres y apellidos completos.
- 2.4.7 La acreditación del requisito de calificación de la experiencia del postor se realiza en base a la documentación aportada por los integrantes del consorcio que se hubieran comprometido a ejecutar conjuntamente las obligaciones vinculadas directamente al objeto materia de la contratación, de acuerdo con lo declarado en la promesa de consorcio. Para ello se debe seguir los siguientes pasos:
- a) Primer paso: obtener el monto de facturación por cada integrante del consorcio, el cual se obtiene de la sumatoria de montos facturados por éste que, a criterio del

evaluador han sido acreditados conforme a las bases, correspondiente a las contrataciones ejecutadas en forma individual y/o consorcio.

En caso un integrante del consorcio presente facturación de contrataciones ejecutadas en consorcio, se considera el monto que corresponda al porcentaje de las obligaciones del referido integrante consorcio. Este porcentaje debe estar consignado expresamente en la promesa o en el contrato de consorcio, de lo contrario, no se considera la experiencia ofertada en consorcio.

- b) Segundo paso: verificar si el integrante del consorcio que acredita la mayor experiencia cumple con un determinado porcentaje de participación. En caso la entidad contratante haya establecido en las bases un porcentaje determinado de participación en la ejecución del contrato, para el integrante del consorcio que acredite mayor experiencia, debe verificarse que éste cumple con dicho parámetro a efectos de considerar su experiencia.
- c) Tercer paso: sumatoria de experiencia de los consorciados. Para obtener la experiencia del consorcio se suma el monto de facturación aportado por cada integrante que cumple con lo señalado previamente.

2.4.8 Para calificar la experiencia del postor no se toma en cuenta la documentación presentada por el o los consorciados que asumen las obligaciones referidas a las siguientes actividades:

- i) Actividades de carácter administrativo o de gestión como facturación, financiamiento, aporte de garantías, entre otras.
- ii) Actividades relacionadas con asuntos de organización interna, tales como representación u otros aspectos que no se relacionan con la ejecución de las prestaciones, entre otras.

2.4.9 Los integrantes del consorcio son responsables de que su inscripción en el RNP se encuentre vigente, así como no estar inhabilitado o suspendido al registrarse como participantes, en la presentación de ofertas, en el otorgamiento de la buena pro y en el perfeccionamiento del contrato.

2.4.10 Los integrantes de un consorcio se encuentran obligados solidariamente a responder frente a la entidad contratante por los efectos patrimoniales que ésta sufra como consecuencia de la actuación de dichos integrantes, ya sea individual o conjunta, durante el procedimiento de selección y la ejecución contractual.

CAPÍTULO III

RECURSO DE APELACIÓN

3.1 ACCESO AL EXPEDIENTE DE CONTRATACIÓN

Una vez otorgada la buena pro, la dependencia encargada de las contrataciones está en la obligación de permitir el acceso de los participantes y postores al expediente de contratación, con excepción de la información calificada como secreta, confidencial o reservada por la normativa de la materia y de aquella correspondiente a las ofertas que no fueron admitidas, a más tardar dentro del día hábil siguiente de haberse solicitado por escrito.

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 contratante debe entregar dicha documentación en el menor tiempo posible, previo pago de la tasa por tal concepto previsto en el Texto Único de Procedimientos Administrativos (TUPA) de la respectiva entidad contratante.

3.2 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, incluyendo aquellos que declaren la nulidad de oficio, la cancelación del procedimiento de selección y otros actos emitidos por la entidad contratante que afecten la continuidad de éste.

El recurso de apelación se presenta ante la mesa de partes digital o física del Tribunal de Contrataciones Públicas y es resuelto por éste.

3.3 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, como máximo, dentro de los ocho (8) días hábiles siguientes de haberse notificado el otorgamiento de la buena pro a través del SEACE de la Pladicop.

En el caso de 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 de selección, el plazo indicado en el párrafo precedente se contabiliza desde que se toma conocimiento del acto que se desea impugnar. Se considera que se ha tomado conocimiento en el día de la publicación en el SEACE de la Pladicop del acto que se desea impugnar.

CAPÍTULO IV DEL CONTRATO

4.1 REQUISITOS PARA EL PERFECCIONAMIENTO DEL CONTRATO:

Para perfeccionar el contrato, el proveedor o proveedores adjudicados presentan los siguientes requisitos de conformidad con el artículo 88 del Reglamento:

REQUISITO	CONSIDERACIONES ADICIONALES	BASE LEGAL
a) Garantías, salvo casos de excepción.	<p>En los contratos de servicios el postor ganador de la buena pro presenta una garantía de fiel cumplimiento por una suma equivalente al 10% del monto del contrato original.</p> <p>La garantía de fiel cumplimiento puede ser: (i) fideicomiso, solo en caso el plazo de ejecución del contrato supere los 90 días calendario, (ii) carta fianza financiera, (iii) contrato de seguro o (iv) retención de pago.</p> <p>Asimismo, en la sección específica de las Bases puede considerarse la presentación de: i) garantía de fiel cumplimiento de prestaciones accesorias y, ii) garantía por adelantos directos, siempre que se cumplan las condiciones señaladas en el Reglamento.</p> <p>La retención de pago como garantía de fiel cumplimiento o de prestaciones accesorias aplica para ítems cuya cuantía adjudicada sea igual o menor a S/ 480 000,00 (cuatrocientos ochenta mil y 00/100 soles). En el caso de las micro y pequeñas empresas estas pueden otorgar como garantía de fiel cumplimiento la retención de pago por parte de la entidad contratante con independencia de la cuantía de la contratación.</p> <p><u>Excepciones:</u> Conforme a lo dispuesto en el literal a) del artículo 139 del Reglamento, en los contratos de bienes y servicios cuyos montos sean menores o iguales a 50 UIT, no corresponde presentar garantía de fiel cumplimiento de contrato ni garantía de fiel cumplimiento por prestaciones accesorias. Esta excepción no aplica cuando la sumatoria de los contratos derivados de procedimientos de selección por relación de ítems, adjudicados a un mismo postor, superen el monto señalado.</p>	<p>Numerales 61.4 y 61.5 del artículo 61 de la Ley.</p> <p>Artículos 88, 113, 114, 115, 116, 138 y 139 del Reglamento.</p>
b) Contrato de consorcio, de ser el caso.	<p>En caso el postor ganador de la buena pro sea un consorcio, el contrato de consorcio se formaliza mediante documento privado con firmas legalizadas de cada uno de los integrantes ante notario público, el cual debe cumplir con los siguientes requisitos:</p>	<p>Literal b) del artículo 88 del Reglamento.</p>

	<p>a. Contener la información mínima indicada en el numeral 2.4.3 del Capítulo II de la Sección General de las presentes bases.</p> <p>b. Identificar al integrante del consorcio a quien se efectuará el pago y emitirá la respectiva factura o, en caso de llevar contabilidad independiente, señalar el Registro Único de Contribuyentes (RUC), del consorcio.</p> <p>c. Consignar las firmas legalizadas ante notario público de cada uno de los integrantes del consorcio, de sus apoderados o de sus representantes legales, según corresponda.</p> <p>Lo indicado no excluye la información adicional que pueda consignarse en el contrato de consorcio con el objeto de regular su administración interna, como es el régimen y los sistemas de participación en los resultados del consorcio, al que se refiere el artículo 448 de la Ley N° 26887, Ley General de Sociedades.</p> <p>En ningún caso puede aceptarse la presentación de la promesa de consorcio que fue parte de la oferta, independientemente de que dicha promesa contenga firmas legalizadas ante notario.</p>	
c) Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de cuenta bancaria y nombre de la entidad bancaria en el exterior.	<p>El CCI es requisito indispensable para realizar una transferencia entre cuentas de bancos diferentes, siendo requerido para efectuar el pago a los proveedores domiciliados en el Perú.</p> <p>Para los proveedores no domiciliados, corresponde el número de cuenta bancaria y nombre de la entidad bancaria en el exterior.</p>	<p>Artículo 67 de la Ley.</p> <p>Artículo 88 del Reglamento.</p>
d) Documento que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.	<p>Corresponde a la vigencia del poder del representante legal que acredite que cuenta con facultades para perfeccionar el contrato. Asimismo, corresponde que el representante legal presente copia de su DNI.</p> <p>En el caso de personas naturales, se solicita la copia del DNI del postor.</p> <p>En el caso de consorcios, estos documentos deben ser presentados por cada uno de los integrantes del consorcio que suscriban la promesa de consorcio, según corresponda.</p>	<p>Literal d) del numeral 88.1 del artículo 88 del Reglamento.</p>

	Asimismo, corresponde se presente copia del DNI del representante común de consorcio	
e) Institución Arbitral elegida por el postor, de corresponder.	Este requisito es obligatorio para todos los contratos que superen las 10 UIT ¹ . Desde el 1 de enero de 2026, la institución arbitral elegida debe encontrarse inscrita en el Registro de Instituciones Arbitrales y Centros de Administración de Juntas de Prevención y Resolución de Disputas (REGAJU).	Artículos 77, 83 y 84, así como la Décima Disposición Complementaria Transitoria de la Ley. Artículo 88 del Reglamento

4.2 PERFECCIONAMIENTO DEL CONTRATO

El postor ganador de la buena pro debe presentar los requisitos para perfeccionar el contrato dentro del plazo de ocho o cinco días hábiles, según corresponda, contabilizados desde el día siguiente al registro del consentimiento de la buena pro en el SEACE de la Pladiscop o de que ésta haya quedado administrativamente firme, de conformidad con el procedimiento y plazos dispuestos en los artículos 88, 89, 90 y 91 del Reglamento.

Cabe indicar que numeral 87.3 del artículo 87 del Reglamento establece que la entidad contratante suscribe el contrato mediante firma digital, en caso de que el postor adjudicado con la buena pro cuente con certificado digital emitido por una entidad de certificación, de acuerdo con la normativa de la materia. Excepcionalmente, la entidad contratante con el debido sustento puede proceder a la firma del contrato mediante medios manuales.

4.3 CONSIDERACIONES PARA LOS CONSORCIOS

4.3.1 Las garantías que presenten los consorcios para el perfeccionamiento del contrato durante la ejecución contractual y para la interposición de los recursos impugnativos, además de cumplir con las condiciones establecidas en la Ley y el 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 pueden ser aceptadas por las entidades contratantes o el Tribunal de Contrataciones Públicas. No se cumple el requisito antes indicado si se consigna únicamente la denominación del consorcio.

4.3.2 Para que un consorcio solicite la retención del 10% del monto del contrato original en calidad de garantía de fiel cumplimiento, según lo señalado en el artículo 114 del Reglamento, todos los integrantes del consorcio deben acreditar en su oferta la condición de micro o pequeña empresa, sin perjuicio que puedan acreditarlo al momento del perfeccionamiento del contrato

4.4 CONSIDERACIONES PARA LAS GARANTÍAS FINANCIERAS

4.4.1 En caso de garantías financieras, estas deben ser incondicionales, solidarias, irrevocables y de realización automática en el país, al solo requerimiento de la respectiva entidad contratante bajo responsabilidad de las empresas que las emiten. Las empresas que emitan garantías financieras deben encontrarse bajo la supervisión directa de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones, contar con clasificación de riesgo B o superior, y 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.

4.4.2 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>).

¹ De conformidad con el numeral 84.1 del artículo 84 de la Ley, el arbitraje puede ser ad hoc solo en los casos en los que el monto de la controversia no supere las diez UIT.

- 4.4.3** 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. Para fines de lo establecido en el artículo 61 de la Ley, se requiere la clasificación de riesgo B o superior.
- 4.4.4** Si la empresa que otorga la garantía cuenta con más de una clasificación de riesgo emitida por distintas empresas listadas en la sede digital de la SBS, basta que en una de ellas cumpla con la clasificación mínima establecida en la Ley.
- 4.4.5** En caso exista alguna duda sobre la clasificación de riesgo asignada a la empresa emisora de la garantía, se debe consultar a la clasificadora de riesgos respectiva.
- 4.4.6** 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 la sede digital de dicha entidad (<http://www.sbs.gob.pe/sistema-financiero/relacion-de-empresas-que-se-encuentran-autorizadas-a-emitir-cartas-fianza>).

4.5 CONSIDERACIONES PARA LOS DOCUMENTOS PÚBLICOS EXTENDIDOS EN EL EXTRANJERO

En el caso que los documentos para el perfeccionamiento del contrato incluyan documentos públicos extendidos en el exterior, que no les sea aplicable el Convenio de la Apostilla, debe tenerse en cuenta que, de conformidad con lo previsto en el artículo 137 del Reglamento Consular del Perú, aprobado mediante Decreto Supremo N° 032-2023-RE², para que estos surtan efectos legales en el Perú deben estar legalizados por los funcionarios consulares peruanos competentes, cuyas firmas deben ser autenticadas posteriormente por el área competente del órgano de línea consular, además de cumplir con los requisitos adicionales que contemple la legislación peruana para su validez en el Perú. Debe considerarse que el mencionado Convenio de la Apostilla contiene definición de documentos públicos.

Cuando se trate de documentos públicos emitidos en países que formen parte del Convenio de la Apostilla, basta con que estos cuenten con la Apostilla de la Haya que el dispositivo normativo establece. Sin perjuicio de lo anterior, se debe cumplir con los requisitos adicionales que contemple la normativa especial de la materia para la validez en el Perú de los documentos extendidos en el exterior.

En el caso de los documentos privados, extendidos en el exterior, estos también deben ser legalizados, conforme es aplicable el artículo 138 del referido del Reglamento Consular del Perú, según el cual el funcionario consular sólo legaliza firmas en documentos privados cuando hayan sido suscritas en su presencia o cuando conste de modo indubitable su autenticidad, verificando en ambos casos la identidad de los firmantes.

4.6 DISPOSICIONES FINALES

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

² Decreto Supremo que aprueba el Reglamento Consular del Perú y que modifica el Reglamento de la Ley del Servicio Diplomático de la República en lo que corresponde a los cargos de los funcionarios consulares.

SECCIÓN ESPECÍFICA

CONDICIONES ESPECIALES DEL PROCEDIMIENTO DE SELECCIÓN

(EN ESTA SECCIÓN LA ENTIDAD CONTRATANTE DEBE COMPLETAR LA INFORMACIÓN EXIGIDA, DE ACUERDO CON
LAS INSTRUCCIONES INDICADAS)

CAPÍTULO I GENERALIDADES

1.1. BASE LEGAL

- Ley N° 32069, Ley General de Contrataciones Públicas.
- Decreto Supremo N° 009-2025-EF, Decreto Supremo que aprueba el Reglamento de la Ley General de Contrataciones Públicas.
- Ley de Presupuesto del Sector Público para el año fiscal 2025.
- Ley de Equilibrio Financiero del Presupuesto del Sector Público del año fiscal 2025.
- Política Nacional de Transformación Digital (PNTD).
- Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD.

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

1.2. ENTIDAD CONTRATANTE

Nombre : CORPORACIÓN PERUANA DE AEROPUERTOS Y AVIACIÓN COMERCIAL - CORPAC S.A.

RUC N° : 20100004675

Domicilio legal : AV. ELMER FAUCETT 3400- AEROPUERTO INTERNACIONAL "JORGE CHÁVEZ", CALLAO.

Teléfono: : (511) 414-1000

Correo electrónico: : tlopez@corpac.gob.pe
acastro@corpac.gob.pe
jhuaman@corpac.gob.pe

1.3. OBJETO DE LA CONVOCATORIA

El presente procedimiento de selección tiene por objeto la contratación de **Servicio de monitoreo y alerta de seguridad – CYBERSOC**.

1.4. CUANTÍA DE LA CONTRATACIÓN³

La cuantía de la contratación no se dará a conocer a los proveedores de conformidad con lo determinado en la estrategia de contratación y lo dispuesto en el numeral 53.4 del artículo 53 del Reglamento.

1.5. EXPEDIENTE DE CONTRATACIÓN

El expediente de contratación fue aprobado el 08 de julio de 2025.

1.6. FUENTE DE FINANCIAMIENTO

Recursos Directamente Recaudados.

³ El monto de la cuantía de la contratación indicado en esta sección de las bases no debe diferir del monto de la cuantía de la contratación consignado en la ficha del procedimiento de selección en el SEACE de la Pladip. No obstante, de existir contradicción entre estos montos, primará el monto de la cuantía de la contratación indicado en las bases aprobadas.

CAPÍTULO II DEL PROCEDIMIENTO DE SELECCIÓN

2.1. CRONOGRAMA DEL PROCEDIMIENTO DE SELECCIÓN

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

2.2. CONTENIDO DE LAS OFERTAS

La oferta contiene, un índice de documentos⁴ y la siguiente documentación:

2.2.1. Documentación de presentación obligatoria

2.2.1.1. Documentos para la admisión de la oferta:

Los evaluadores verifican la presentación de los documentos señalados en el presente acápite. De no cumplir con lo requerido, la oferta se considera no admitida. Los evaluadores no pueden incorporar documentos adicionales para la admisión de la oferta a los establecidos en este acápite.

- a) Declaración jurada de datos del postor. (**Anexo N° 1**)
- b) Pacto de integridad (**Anexo N° 2**)
- c) 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, estos documentos deben ser presentados por cada uno de los integrantes del consorcio que suscriban la promesa de consorcio, según corresponda.

Advertencia

De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, Decreto Legislativo que aprueba diversas medidas de simplificación administrativa, las entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la entidad contratante es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE⁵ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir el certificado de vigencia de poder y/o documento nacional de identidad.

- d) Declaración jurada declarando que: (i) es responsable de la veracidad de los documentos e información de la oferta, y (ii) no se encuentra impedido para contratar con el Estado, de acuerdo con el artículo 33 de la Ley. (**Anexo N° 3**)
- e) Promesa de consorcio con firmas digitales, o en su defecto, firmas legalizadas, de

⁴ La omisión del índice no determina la no admisión de la oferta.

⁵ Para mayor información de las Entidades usuarias y del Catálogo de Servicios de la Plataforma Nacional de Interoperabilidad – PIDE ingresar al siguiente enlace <https://www.gob.pe/741-plataforma-nacional-de-interoperabilidad>

ser el caso, en la que se consigne los integrantes, el representante común, el domicilio común, el correo electrónico 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° 4**)

- f) Documentación que acredite la desafectación del impedimento, en caso el proveedor al registrarse como participante hubiera presentado la Declaración Jurada de Desafectación del Impedimento (**Anexo N° 5**), de conformidad con el numeral 39.4 del artículo 39 del Reglamento.

Advertencia

El requisito indicado en el literal f) únicamente se solicitará al proveedor que al registrarse hubiera presentado la Declaración Jurada de Desafectación del Impedimento.

- g) Oferta Económica (**Anexo N° 6**). En caso el requerimiento contenga prestaciones accesorias, la oferta económica individualiza los montos correspondientes a las prestaciones principales y las prestaciones accesorias.

En el caso de compras corporativas, los postores deben formular su oferta económica de manera individual por cada entidad contratante.

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 3.5 del Capítulo III de la presente sección de las bases.

2.2.2. Documentación de presentación facultativa

- 2.2.2.1.** Incorporar en la oferta los documentos que acreditan los “**Factores de Evaluación**” establecidos en el Capítulo IV de la presente sección de las bases, a efectos de obtener el puntaje previsto en dicho Capítulo para cada factor.

Advertencia

Los evaluadores no pueden exigir al postor la presentación de documentos que no hayan sido indicados en los acápites “Documentos para la admisión de la oferta”, “Requisitos de calificación” y “Factores de evaluación”.

2.3. REQUISITOS PARA PERFECCIONAR EL CONTRATO

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

- Garantía de fiel cumplimiento del contrato, autorización de retención (**Anexo N° 7**) o declaración jurada comprometiéndose a presentar la garantía mediante fideicomiso (**Anexo N° 8**), de ser el caso.
- Contrato de consorcio con firmas legalizadas ante notario de cada uno de los integrantes, de ser el caso.
- Código de cuenta interbancaria (CCI) o, en el caso de proveedores no domiciliados, el número de su cuenta bancaria y nombre de la entidad bancaria en el exterior.
- Copia de la vigencia del poder del representante legal del postor que acredite que cuenta con facultades para perfeccionar el contrato, cuando corresponda.
- Copia de DNI del postor en caso de persona natural o de su representante legal en caso de persona jurídica.
- Autorización de notificaciones durante la ejecución del contrato al correo electrónico contemplado en el contrato (**Anexo N° 9**).

- g) Institución Arbitral elegida por el postor (**Anexo N° 10**).

Advertencia

La Institución Arbitral es elegida por el postor ganador de la buena pro de la lista de instituciones arbitrales que haya propuesto la entidad contratante en las bases del procedimiento de selección. Para dicho efecto, al remitir los documentos para la suscripción del contrato, el postor ganador de la buena pro comunica a la entidad contratante la Institución Arbitral elegida de la referida lista, caso contrario, acuerda con la entidad contratante una Institución Arbitral distinta. En caso de falta de acuerdo, la Institución Arbitral es elegida de la mencionada lista por la entidad contratante de manera definitiva. Las partes pueden establecer estipulaciones adicionales o modificatorias del convenio arbitral, en la medida que no contravengan las disposiciones de la normativa de contrataciones públicas y/o las disposiciones especiales contenidas en la normativa general de arbitraje.

- h) Normas y certificaciones: ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27701:2019 y Certificación CSA STAR CCM v4.0, de acuerdo con lo detallado en el numeral 5.1.1.1. de los términos de referencia.
- i) Seguros del Operador de Sitio que estará in situ en las instalaciones de CORPAC, de acuerdo con lo detallado en el numeral 5.4. de los términos de referencia.
- j) Evidencia de por lo menos quince (15) auditorías realizadas a diferentes empresas del personal clave requerido como LIDER DEL PROYECTO Y RESPONSABLE DE LA AUDITORIA Y CUMPLIMIENTO DE LA NORMA ISO27001:2022 – EXTERNO, de acuerdo con lo detallado en el numeral 6.3. de los términos de referencia (A. Personal clave).
- k) Certificaciones del personal clave, de acuerdo con lo detallado en el numeral 6.3. de los términos de referencia (A. Personal clave).
- l) Declaración Jurada Actualizada de Desafectación de Impedimento (**Anexo N° 15**) y la documentación que acredite dicha desafectación.
- m) Declaración Jurada sobre Inaplicación del Impedimento Tipo 4.D del inciso 4 del numeral 30.1 del Artículo 30 de La Ley N° 32069 Referido a La Inscripción en el Registro de Deudores Alimentarios Morosos – Redam; (**Anexo N° 18**), de ser el caso.

Advertencia

- El requisito indicado en el literal l) únicamente se solicitará si el postor adjudicado hubiera presentado la Declaración Jurada de Desafectación del Impedimento en el procedimiento de selección.*
- De acuerdo con el artículo 4 del Decreto Legislativo N° 1246, las entidades están prohibidas de exigir a los administrados o usuarios la información que puedan obtener directamente mediante la interoperabilidad a que se refieren los artículos 2 y 3 de dicho Decreto Legislativo. En esa medida, si la entidad contratante es usuaria de la Plataforma de Interoperabilidad del Estado – PIDE⁶ y siempre que el servicio web se encuentre activo en el Catálogo de Servicios de dicha plataforma, no corresponderá exigir los documentos previstos en los literales e) y f) del presente numeral.*
- En caso el postor declare la inaplicabilidad del impedimento Tipo 4.D del inciso 4 del numeral 30.1 del artículo 30 de la Ley, referido a las personas inscritas en el Registro de Deudores Alimentarios Morosos del Poder Judicial (REDAM) presenta la Declaración Jurada respectiva (Anexo N° 18).*

2.4. PERFECCIONAMIENTO DEL CONTRATO

2.4.1 El contrato se perfecciona con la suscripción del documento que lo contiene. La entidad contratante suscribe el contrato mediante firma digital, en caso de que el postor adjudicado con la buena pro cuente con certificado digital emitido por una entidad de certificación, de acuerdo con la normativa de la materia. Excepcionalmente, la entidad contratante con el debido sustento puede proceder a la firma del contrato mediante medios manuales.

⁶ Para mayor información de las entidades usuarias y del Catálogo de Servicios de la Plataforma de Interoperabilidad del Estado – PIDE ingresar al siguiente enlace <https://www.gob.pe/741-plataforma-nacional-de-interoperabilidad>

2.4.2 El contrato firmado digitalmente se remite a la siguiente dirección electrónica: ylflores@corpac.gob.pe; mcastillo@corpac.gob.pe, ccuyam@corpac.pe, en caso de no contar con firma digital, la suscripción del contrato se realiza en el Área de Contratos de la Gerencia de Logística, en Calle Corpac S/N Callao.

2.5. FORMA DE PAGO

El pago se realiza de conformidad con lo establecido en el artículo 67 de la Ley.

La entidad contratante paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días hábiles siguientes de otorgada la conformidad por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles.

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

La entidad contratante realiza el pago de la contraprestación pactada a favor del contratista en PAGOS MENSUALES, se realizará cada 30 días por los 1095 días calendarios, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

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

- Documento en el que conste la conformidad de la prestación efectuada suscrita por el servidor responsable del Área de Redes, Comunicaciones y Soporte Técnico y la Gerencia de Tecnología de la Información y comunicaciones de CORPAC.
- Comprobante de pago.
- Informe del CONTRATISTA del mes correspondiente.

Se precisa que la documentación debe ser presentada por el contratista es conforme lo siguiente:

Para el primer pago la Entidad deberá de contar con:

- Comprobante de pago
- Informe del contratista del entregable correspondiente
- Acta de conformidad por parte de la entidad
- Presentación del plan de trabajo
- Informe de implementación.

Para el segundo pago, la entidad deberá de contar con:

- Comprobante de pago
- Informe del contratista del entregable correspondiente
- Acta de conformidad por parte de la entidad
- Acta de finalización del taller y/o curso.

Para el tercer y hasta el último pago la Entidad deberá de contar con:

- Comprobante de pago
- Informe del contratista del mes correspondiente
- Acta de conformidad por parte de la entidad del mes correspondiente
- informe final de resultados, estadísticas e incidentes gestionados (ultimo pago).

En caso de retraso en el pago por parte de la Entidad, salvo que se deba acaso fortuito o fuerza mayor, EL CONTRATISTA tiene derecho al pago de intereses legales conforme a lo establecido en el artículo 67 de la Ley N° 32069, Ley General de Contrataciones Públicas.

Salvo los documentos que emite la entidad contratante, es decir, de recepción y verificación, así

como de conformidad, el contratista debe presentar la documentación restante a través de la Mesa de Partes Virtual de CORPAC S.A., dentro de los horarios de trabajo establecidos 8:30 a 16:30 horas. Pasado dicho horario, los usuarios pueden presentar documentación, pero se dará por recibida a partir del día hábil siguiente. Enlace mesa de partes virtual: [https://extranet.corpac.gob.pe/mesapartesvirtual/"Account/Login?ReturnUrl=%2Fmesa-partes-virtual%2F](https://extranet.corpac.gob.pe/mesapartesvirtual/)

Advertencia

En caso se verifique que el proveedor tiene multas impagas que no se encuentren en procedimiento coactivo, se incorpora al contrato una cláusula de compromiso de pago de la multa, estableciéndose que durante la ejecución del contrato la entidad contratante retiene de forma prorrateada hasta el 10% del monto del contrato, para el pago o amortización de multas.

CAPÍTULO III REQUERIMIENTO

Advertencia

Al elaborar las bases, los evaluadores incluyen en esta sección el requerimiento que forma parte del expediente de contratación aprobado. El área usuaria es responsable de formular adecuadamente el requerimiento, en coordinación con la dependencia encargada de las contrataciones, de conformidad con el artículo 20 del Reglamento. El requerimiento debe elaborarse de acuerdo con el formato consignado en este capítulo y estar incluido en el cuadro multianual de necesidades.

3.1. FINALIDAD PÚBLICA DE LA CONTRATACIÓN

Contratar un SERVICIO DE MONITOREO Y ALERTA DE SEGURIDAD - CYBERSOC brindado a través de un CyberSOC administrado, esto debido a que el cibercrimen ha alcanzado niveles de sofisticación sin precedentes, y la digitalización en las empresas las dejan expuestas a una amplia variedad de nuevas amenazas: ataques masivos de ransomware, estafas de phishing, robo de información, y más. Estos delitos podrían ocasionar una gran afectación a CORPAC y todos sus grupos de interés.

La mejor práctica para combatir esta ola de cibercrimen es contar con un Centro de Operaciones de Seguridad Cibernético (Cyber Security Operations Center - CyberSOC). Se propone, mantener una gestión preventiva a través del trabajo efectivo de un equipo especializado en realizar ejercicios de hacking ético que revelen y detallen de manera oportuna huecos de seguridad, vulnerabilidades y configuraciones débiles que los ciberdelincuentes puedan aprovechar para atentar sobre los sistemas, además de un equipo de expertos en seguridad responsables de monitorear eventos, anomalías y posibles amenazas las 24 horas del día, los 7 días de la semana, utilizando tecnología de punta para detectar y responder a ataques en tiempo real.

Dado que el poseer y mantener un CyberSOC es costoso, complejo y fuera del objeto de negocio de CORPAC S.A. El SERVICIO DE MONITOREO Y ALERTA DE SEGURIDAD - CYBERSOC brindado a través de un CyberSOC administrado, deberá ofrecer en conjunto estrategias y acciones preventivas para que esta corporación pueda lograr óptimos niveles en detección y respuesta ante amenazas.

Con la contratación del servicio se busca que la corporación cuente con una asistencia integral de seguridad preventiva y reactiva, que permita reducir la superficie de ataque externa e interna de CORPAC S.A., efectuando un monitoreo permanente de su plataforma, con la consiguiente disminución del riesgo.

Por otro lado, la plataforma del CyberSOC solicitada debe tener una arquitectura de administración compartida permitiendo el acceso total a personal de CORPAC S.A. considerando capacidades de tratamiento de eventos, integraciones, así como el detalle de análisis forense que se aplique a cada activo protegido.

3.2. DESCRIPCIÓN GENERAL DEL REQUERIMIENTO

Ítem	Cantidad	Descripción del servicio
1	01	<p>SERVICIO DE MONITOREO Y ALERTA DE SEGURIDAD - CYBERSOC brindado a través de un CyberSOC administrado, deberá permitir la administración efectiva de los equipos de trabajo de CORPAC, el CONTRATISTA y el fabricante.</p> <p>El servicio deberá ejecutarse por un periodo de mil noventa y cinco (1095) días calendario garantizando la prevención, detección, análisis e investigación y respuesta ante incidentes de ciberseguridad y reacción efectiva ante ataques cibernéticos sobre un total de ciento veinte (120) servidores, mil cuatrocientos</p>

		cincuenta (1450) estaciones de trabajo a nivel nacional, dos (02) firewalls, cuatro (04) switches Core/Distribución, setenta (70) Routers, cuarenta (40) Switches, un (01) sistema de correo y antispam y un (01) WAF, integrando a nivel de API y correlacionado las fuentes de antivirus, EDR, XDR, antispam, correo, firewalls, switches u otros componentes de red, para mejorar la tasa de detección y respuesta.
--	--	--

3.3. CONDICIONES DE CONTRATACIÓN

a. MODALIDAD DE PAGO

El contrato se rige por la modalidad de SUMA ALZADA, de conformidad con el artículo 130 del Reglamento.

b. SISTEMA DE ENTREGA

No aplica.

c. PLAZO DE PRESTACIÓN

A continuación, se detallan los plazos correspondientes a cada etapa del servicio:

Plazo para el plan de trabajo

El plazo máximo para esta etapa es de cinco (5) días calendarios, contabilizados a partir del día siguiente de la firma del contrato

Plazo de Implementación del Servicio:

El plazo máximo para esta etapa es de treinta (30) días calendarios contabilizados a partir del día siguiente de suscrito la conformidad del Primer entregable que es el Plan de Trabajo.

Plazo de Operación del Servicio:

El plazo para la ejecución del servicio en su etapa operativa es de mil noventa y cinco (1095) días calendario, contabilizados a partir del día siguiente de la suscripción del Acta de inicio de la Etapa de Operación del Servicio, una vez culminada satisfactoriamente la etapa de implementación.

Dentro de ese plazo, también se realizará:

- Servicio integral para la mejora de la seguridad de la información y ciberseguridad según la NIST CSF 2.0 o NIST IR 8376.
- Dentro de los 30 días calendarios posteriores de la implementación del CyberSOC se presentará el primer informe de cumplimiento.
- Servicio de operación análisis de ciberseguridad IN-SITU
Dentro de los 10 días calendarios, posteriores de la implementación del CyberSOC iniciaría formalmente el analista responsable en los horarios establecidos por la vigencia del contrato.
- Ejercicios de HACKING ÉTICO con remediación integral asistida de forma trimestral a través de la plataforma de gestión colaborativa segura.
 1. Dentro de los 30 días calendarios posteriores de la implementación del CyberSOC se presentaría formalmente el primer ejercicio de hacking ético con remediación asistida.
 2. El ejercicio deberá ejecutarse tres (03) veces al año, y deberá mantener activo detalles de los ejercicios y remediaciones en una plataforma de gestión colaborativa segura durante la vigencia del contrato.

C) Plazo de Cierre del Servicio:

El plazo para la etapa de cierre tendrá una duración de sesenta días (60) calendarios como máximo, dentro de la Etapa de Operación del Servicio.

d. LUGAR DE PRESTACIÓN DE SERVICIO

La ejecución del servicio se realizará en la sede central de CORPAC S.A ubicada en la Av. Elmer Faucett N° 3400 Aeropuerto Internacional Jorge Chavez Zona Sur. (Edificio Ex OACI).

e. ADELANTOS

No corresponde.

f. PENALIDADES

PENALIDAD POR MORA:

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable, de conformidad con el artículo 120 del Reglamento.

OTRAS PENALIDADES:

Adicionalmente a la penalidad por mora, se aplicarán las siguientes penalidades:

Otras Penalidades			
N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
1	Realizar cambios de personal asignado al servicio, sin contar con la aprobación de la Gerencia de Tecnología de la Información y Comunicaciones	10% de la UIT. Se aplicará la penalidad por cada ocurrencia	Mediante informe de la Gerencia de Tecnología de la Información y Comunicaciones, la cual supervisará el servicio.

Por incumplimientos de Niveles de Servicio (SLA)

Penalizaciones en SERVICIOS DE CYBERSOC		
Servicio	SLA	Penalidad
Monitoreo de salud de la plataforma	Disponibilidad diaria 24x7x365	Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.
Monitoreo avanzado tiempo real y correlación de eventos de seguridad	Disponibilidad diaria 24x7x365	Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.

Cyber Threat Intelligence (Inteligencia de Ciberseguridad)	Disponibilidad diaria 24x7x365	Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.			
Threat Hunting	Disponibilidad diaria 24x7x365	Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.			
Alerta Temprana	Disponibilidad diaria 24x7x365	Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.			
Portal de Supervisión	Disponibilidad diaria 24x7x365	Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.			
Penalizaciones en Advanced Security Incident Response (Respuesta Avanzada a Incidentes)					
Registro de incidente: Ticket generado por CONTRATISTA	Tiempo promedio de detección e inicio del análisis	Tiempo promedio de contención	Tiempo promedio de reparación	Tiempo promedio de resolución	Análisis de repercusiones
<= 15 minutos de reportado el incidente	< 30 minutos	< 45 minutos	< 3 horas	< 6 horas	Dentro de las 48 horas de resuelto el incidente.

Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	Penalidad : 3% de UIT por cada ocurrencia de incumplimiento	Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	Penalida d: 3% de UIT por cada ocurrencia de incumplimiento
Penalidades por Tiempos de Atención Off-Site					
Disponibilidad 24 x 7 x 365			Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.		
2 horas de atención como plazo máximo en Lima Metropolitana			Penalidad: 3% de UIT por cada ocurrencia de incumplimiento		
4 horas de atención como plazo máximo en provincias			Penalidad: 3% de UIT por cada ocurrencia de incumplimiento		
Penalidades por Registro de tickets de mesa de ayuda					
Tiempo máximo de registro del incidente, desde que son reportados		15 minutos		Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	

La suma de la aplicación de las penalidades por mora y otras penalidades no debe exceder el 10% del monto vigente del contrato, de ser el caso, del ítem correspondiente.

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

g. SUBCONTRATACIÓN

Se encuentra prohibida la subcontratación de las prestaciones objeto del contrato.

h. FÓRMULAS DE REAJUSTES

No corresponde.

i. SOLUCIÓN DE CONTROVERSIAS CONTRACTUALES

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, cuando se haya pactado y arbitraje.

Para el arbitraje, el postor ganador de la buena pro selecciona a una de las siguientes Instituciones Arbitrales para administrar el arbitraje:

- Centro de Arbitraje del OSCE – Organismo Supervisor de las Contrataciones del Estado
- Centro de Análisis y Resolución de Conflictos -PUCP.
- Centro de Arbitraje de la cámara de Comercio de Lima.

3.4. TÉRMINOS NOS DE REFERENCIA



Firmado Digitalmente por:
AYBAR CARMONA Jerson
Jesús FAU 2010004675 soft
Razón: VISTO BUENO
Fecha: 17/06/2025 11:04:05

Requerimiento Términos de Referencia



Firmado Digitalmente por:
JULIO CESAR BENAVIDES
ARBULU
Motivo: SUSCRITO
Fecha: 17/06/2025 11:08:35

Denominación de la Contratación	SERVICIO DE MONITOREO Y ALERTA DE SEGURIDAD
Actividad del POI	<p>El servicio de monitoreo y alerta de seguridad cybersoc an ciberseguridad se enmarca en la acción estratégica AEI 9.2: "Implementación de la Unidad de Seguridad de la Información", alineada con el Objetivo Estratégico: "Implementar el Gobierno y la Transformación Digital de la empresa".</p> <p>Esta iniciativa tiene como propósito fortalecer la postura de seguridad de los sistemas informáticos de CORPAC a nivel nacional mediante la implementación de un servicio integral de monitoreo 24x7 de la infraestructura tecnológica. Dicho servicio permitirá identificar y neutralizar amenazas de manera proactiva, asegurando la protección de datos sensibles y garantizando la continuidad operativa. La adopción de tecnologías avanzadas en ciberseguridad, junto con la integración de herramientas de gestión de incidentes, optimizará la capacidad de respuesta ante ataques y contribuirá significativamente a la transformación digital de la institución.</p>
Área Usuaría	Área de Redes, Comunicaciones y Soporte Técnico

1. Finalidad Pública

Contratar un SERVICIO DE MONITOREO Y ALERTA DE SEGURIDAD - CYBERSOC brindado a través de un CyberSOC administrado, esto debido a que el cibercrimen ha alcanzado niveles de sofisticación sin precedentes, y la digitalización en las empresas las dejan expuestas a una amplia variedad de nuevas amenazas: ataques masivos de ransomware, estafas de phishing, robo de información, y más. Estos delitos podrían ocasionar una gran afectación a CORPAC y todos sus grupos de interés.

La mejor práctica para combatir esta ola de cibercrimen es contar con un Centro de Operaciones de Seguridad Cibernético (Cyber Security Operations Center - CyberSOC). Se propone, mantener una gestión preventiva a través del trabajo efectivo de un equipo especializado en realizar ejercicios de hacking ético que revelen y detallen de manera oportuna huecos de seguridad, vulnerabilidades y configuraciones débiles que los ciberdelincuentes puedan aprovechar para atentar sobre los sistemas, además de un equipo de expertos en seguridad responsables de monitorear eventos, anomalías y posibles amenazas las 24 horas del día, los 7 días de la semana, utilizando tecnología de punta para detectar y responder a ataques en tiempo real.

Dado que el poseer y mantener un CyberSOC es costoso, complejo y fuera del objeto de negocio de CORPAC S.A. El SERVICIO DE MONITOREO Y ALERTA DE SEGURIDAD - CYBERSOC brindado a través de un CyberSOC administrado, deberá ofrecer en conjunto estrategias y acciones preventivas para que esta corporación pueda lograr óptimos niveles en detección y respuesta ante amenazas.

Con la contratación del servicio se busca que la corporación cuente con una asistencia integral de seguridad preventiva y reactiva, que permita reducir la superficie de ataque externa e interna de CORPAC S.A., efectuando un monitoreo permanente de su plataforma, con la consiguiente disminución del riesgo.



Por otro lado, la plataforma del CyberSOC solicitada debe tener una arquitectura de administración compartida permitiendo el acceso total a personal de CORPAC S.A. considerando capacidades de tratamiento de eventos, integraciones, así como el detalle de análisis forense que se aplique a cada activo protegido.

2. Antecedentes

CORPAC S.A. está inmersa en un proceso de transformación digital que busca optimizar sus operaciones y servicios. En este marco, la ciberseguridad se ha consolidado como una prioridad estratégica, orientada a mitigar riesgos asociados a amenazas cibernéticas que puedan comprometer la integridad de la información y la continuidad de las operaciones. La implementación de un servicio integral de monitoreo, prevención, detección, análisis e investigación, y respuesta ante incidentes de ciberseguridad, mediante un CyberSOC coadministrado, es esencial para fortalecer la postura de seguridad de la corporación y garantizar la protección de sus activos digitales.

CORPAC S.A., a través de la licitación pública LP-SM-6-2024-CORPAC S.A.-1, ha adquirido y mantiene activas licencias de "Antivirus Corporativo" con capacidades de Detección y Respuesta Extendida (XDR), operando sobre la plataforma Bitdefender GravityZone. Esta solución nativa de XDR proporciona una visibilidad integral de las amenazas, correlacionando eventos de seguridad a lo largo de la infraestructura tecnológica y facilitando una respuesta automatizada y guiada ante incidentes.

El servicio de monitoreo y alerta de seguridad cybersoc 24x7, Prevención, Detección, Análisis e Investigación y respuesta ante incidentes de ciberseguridad deberá integrarse de manera eficiente con las licencias actuales, permitiendo la ingestión de eventos de seguridad y telemetría generados por la plataforma XDR. Esta integración potenciará la capacidad de detección temprana, optimizará la respuesta ante incidentes y fortalecerá la postura de seguridad de CORPAC S.A., alineándose con las mejores prácticas en ciberseguridad.

Como parte de la Política Nacional de Transformación Digital (PNTD), se tienen lineamientos a ser implementados en materia de la Seguridad de la Información. Es así como, mediante la resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023- PCM/SGTD se establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas. A fin de coadyuvar con dicha política, CORPAC necesita garantizar que sus activos de información no se vean afectados por agentes de amenaza externa, es por esto por lo que se requiere contratar un servicio de monitoreo y alerta de seguridad cybersoc brindado a través de un CyberSOC administrado, garantizando así EFICIENCIA y EFICACIA de procesos de seguridad informática para la Infraestructura de TI, Sistemas y Aplicaciones de CORPAC.

El presente requerimiento no cuenta con contratación histórica.

3. Objetivo de la Contratación

3.1 Objetivo General

Contar con un servicio especializado que garantice un monitoreo efectivo y permanente 24x7 por parte de especialistas, documentando eventos de seguridad de múltiples fuentes en tiempo real desde una plataforma de CyberSOC administrada con el fin de detectar oportunamente los riesgos que derivan de ataques cibernéticos.

El servicio debe estar en condiciones de:

- Prevenir un ciberataque a través de la ejecución periódica y recurrente de ejercicios de hacking ético y la reducción efectiva de la superficie de ataque interna y externa.
- Detectar y responder ante un incidente a través de la correlación efectiva de todos los eventos relacionados a diversas fuentes como correo, antivirus, servidores, estaciones, firewall y/o dispositivos de comunicación.



- Documentar y madurar un framework de seguridad en el tiempo que permita medir objetivamente como se reduce el nivel de exposición al riesgo en el tiempo.

El objetivo principal consiste en implementar y madurar un estándar y/o framework de seguridad que permita reducir objetivamente el nivel de riesgo cibernético en CORPAC S.A., aprovechando el feedback que generan los servicios y plataformas de seguridad que componen la solución ofertada.

3.2 Objetivo Específico

- Implementar un marco de ciberseguridad NIST CSF 2.0 que permita establecer un plan de tratamiento viable en el tiempo basado en objetivos específicos que permitan evidenciar una eficiente y eficaz gestión de riesgos de ciberseguridad.
- Implementar capacidades de prevención de riesgos a través de la ejecución recurrente de ejercicios de hacking ético y sensores de análisis continuo que permitan:
 - Reconocer, priorización y reducir riesgos cibernéticos de forma continua sobre la superficie de ataque externa de CORPAC S.A.
 - Reconocer, priorización y reducir riesgos cibernéticos de forma continua sobre la superficie de ataque interna de CORPAC S.A.
 - Mantener un monitoreo continuo que ayuden a predecir ataques cibernéticos dirigidos hacia la RED de CORPAC a través del monitoreo activos de la dark web y los canales más utilizados por hackers y ciberdelinquentes.
- Implementar capacidades de detección y respuesta 24x7, sobre los activos de misión crítica en CORPAC S.A., integrando:
 - El correlacionamiento de eventos de las plataformas relevantes como estaciones estratégicas, servidores, firewalls, componentes de red y correo electrónico.
 - Analizando en tiempo real técnicas de ataque, archivos y eventos sospechosos con la finalidad de responder aislando un recurso en el momento que se configure el ataque.
- Documentar la mejora de postura de seguridad en el tiempo a través de la implementación y mantenimiento del framework de seguridad NIST, asistiendo de forma integral el proceso de determinación de acciones, definición de responsabilidades y medición del nivel de madurez de los controles implementados en el tiempo.

4. BASE LEGAL

- Ley N° 32069, Ley General de Contrataciones Públicas.
- Decreto Supremo N° 009-2025-EF, Decreto Supremo que aprueba el Reglamento de la Ley General de Contrataciones Públicas.
- Política Nacional de Transformación Digital (PNTD).
- Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD.

5. CARACTERÍSTICAS Y CONDICIONES DEL SERVICIO A CONTRATAR

5.1. Descripción del Servicio a contratar

Ítem	Cantidad	Descripción del servicio
1	01	<p>SERVICIO DE MONITOREO Y ALERTA DE SEGURIDAD - CYBERSOC brindado a través de un CyberSOC administrado, deberá permitir la administración efectiva de los equipos de trabajo de CORPAC, el CONTRATISTA y el fabricante.</p> <p>El servicio deberá ejecutarse por un periodo de mil noventa y cinco (1095) días calendario garantizando la prevención, detección, análisis e investigación y respuesta ante incidentes de ciberseguridad y reacción efectiva ante ataques cibernéticos sobre un total de ciento veinte (120) servidores, mil cuatrocientos cincuenta (1450) estaciones de trabajo a nivel</p>



	nacional, dos (02) firewalls, cuatro (04) switches Core/Distribución, setenta (70) Routers, cuarenta (40) Switches, un (01) sistema de correo y antispam y un (01) WAF, integrando a nivel de API y correlacionado las fuentes de antivirus, EDR, XDR, antispam, correo, firewalls, switches u otros componentes de red, para mejorar la tasa de detección y respuesta.
--	---

5.1.1 ACTIVIDADES - ALCANCES Y DESCRIPCIÓN DEL SERVICIO

5.1.1.1. ARQUITECTURA Y PRESENTACIÓN DEL SERVICIO:

- La plataforma de CyberSOC con administración delegada debe ser provista en modalidad de Security as a Service (SECaaS).
- La plataforma de Cyber SOC administrada debe ser provista desde una data center o centro de control operando desde una nube delegada o privada que cuente con las condiciones idóneas para garantizar la continuidad del servicio de ciberseguridad brindados por lo que se demanda mínimamente la certificación de conformidad con las normas:

ISO/IEC 27001:2022, ISO/IEC 27017:2015, ISO/IEC 27701:2019 y Certificación CSA STAR CCM v4.0.

El requerimiento de las normas ISO y certificaciones asociadas establecerá un marco robusto de condiciones y directrices para la adecuada implementación de un sistema de gestión de la seguridad de la información, tanto en plataformas digitales como en entornos cloud. Esto facilitará la aplicación de un proceso riguroso de gestión y control de riesgos, alineado con los requerimientos específicos de la organización, garantizando así una administración eficiente y segura de la información sensible de CORPAC S.A. — incluyendo el tratamiento de datos confidenciales cuya exposición podría comprometer la integridad y seguridad corporativa.

Estas exigencias deberán de ser presentadas para la firma del contrato.

- El fabricante de la plataforma ofertada de CyberSOC debe adjuntar reporte de auditoría de tipo SOC 2 y SOC 3 para los productos base ofertados de manera mensual adjuntado al trámite de pago al área de redes comunicaciones y soporte técnico.
- La plataforma de CyberSOC administrada deberá soportar mínimamente las siguientes plataformas de sistemas operativos Windows 8.1 / Server 2012 R2 (32-bit / 64-bit), Windows 10 / Server 2016 / 2019 (32-bit / 64-bit), Windows 11 / Server 2022 (32-bit / 64-bit), Centos 7 and greater, Ubuntu 18.0 and greater, Red Hat 8 and 9, AWS Linux versión 2.0, macOS Catalina 10.15, macOS Big Sur 11.x, macOS Monterey 12.x y macOS Ventura 13.x.
- La plataforma de CyberSOC administrada debe presentarse como un sistema integrado tipo SOAR integrando tecnologías y plataformas requeridas que se gobiernen desde una sola consola de orquestación automatizada con acceso basado en roles que permita la ADMINISTRACIÓN por parte del equipo de la Corporación, es decir, contar con un usuario que permita la supervisión y monitoreo total de la plataforma propuesta.



- La plataforma de CyberSOC administrada debe proveer capacidades de detección y respuesta administrada con monitoreo activo 24x7 a través del equipo del fabricante permitiendo la eficiencia y efectividad del proceso.
- La plataforma de CyberSOC administrada debe permitir la integración con la infraestructura de TI y seguridad existente, logrando que la plataforma administrada por el equipo de analistas de SOC del fabricante identifique rápidamente actividades maliciosas y sospechosas en los principales vectores de amenazas críticas: endpoint, red y nube, para brindar una defensa avanzada contra ciberamenazas las 24 horas, los 7 días de la semana durante el tiempo que dure la suscripción.
- La plataforma de CyberSOC administrada deberá trabajar preferentemente sobre un esquema basado en agente, el cual solo demande del acceso seguro a una plataforma de CyberSOC gestionada la cual opere desde una data center en nube delegada que cuente con certificaciones y estándares de seguridad propios de la industria.
- La plataforma de CyberSOC administrada debe proporcionar una capacidad segura, liviana y fácil de implementar para capturar la telemetría de seguridad desde los puntos finales a través de un agente ligero que no supere los ocho (08) MB de tamaño a fin de que el equipo de profesionales que trabaja en el SOC Data Center clasifique, correlacione y registre datos de forma eficiente y efectiva.
- La plataforma de CyberSOC administrada debe garantizar la seguridad de la información del activo protegido a través de la configuración de un agente que no pueda aceptar conexión entrante, que no sea compatible con el control remoto, ni con la capacidad de ejecutar contenido generado por el usuario en endpoints (puntos finales) o servidores.
- La plataforma de CyberSOC administrada debe garantizar la seguridad de las comunicaciones usando el protocolo TLS v1.2 permitiendo solo los siguientes conjuntos de cifrado fuertes:
 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256,
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
 - TLS_RSA_WITH_AES_128_GCM_SHA256,
 - TLS_RSA_WITH_AES_256_GCM_SHA384.
- La plataforma de CyberSOC administrada debe admitir la autenticación de dos factores (2FA) para salvaguardar el acceso a la consola.
- La plataforma de CyberSOC administrada debe permitir la coadministración efectiva por parte de la INSTITUCIÓN a través de la integración de un sistema de acceso basado en roles considerando mínimamente:
 - Rol de propietario, habilitando control total sobre la plataforma
 - Rol visualizador, habilitando funciones de seguimiento y generación de informes sobre todos los eventos generados y procesados
 - Rol resolutor de incidentes, habilitando funciones de seguimiento, generación de informes, aislamiento y liberación de host afectados.



- La plataforma de CyberSOC administrada debe poder definir una relación de usuarios que serán notificados a través de correo electrónico y/o vía telefónica específicamente sobre:
 - Amenazas críticas o emergencias en el momento que ocurran.
 - Instrucciones de remediación y/o fortalecimiento de configuraciones.
 - Advertencia y/o detección de vulnerabilidades y/o riesgos latentes.
- La plataforma de CyberSOC administrada debe integrar preferentemente capacidades de SIEM Less para el monitoreo y correlacionamiento de eventos de seguridad de hosts, firewalls, antivirus, directorio activo, correo electrónico y/o componentes de red, incorporando la detección de infracciones basadas en las técnicas de Mitre Attack, la actividad y los servicios de la red, las herramientas sospechosas y la detección de archivos maliciosos para brindar una solución de seguridad integral.
- La plataforma de CyberSOC administrada debe contar con una aplicación que brinde la posibilidad de recopilar y analizar eventos en CEF (formato de evento común) y LEEF (formato extendido de evento de registro) a través de Syslog.
- La plataforma de CyberSOC administrada debe tener una arquitectura multitenant que le permita crear instancias de gobierno independiente asignadas a usuarios clave dentro de la organización.
- La plataforma de CyberSOC administrada debe permitir crear reportes bajo demanda y programarlos para su envío automático al correo electrónico.
- La plataforma de CyberSOC administrada debe permitir la creación de informes de inventario e informes ejecutivos hasta con una antigüedad de noventa (90) días calendarios.
- La plataforma de CyberSOC administrada debe almacenar la información de eventos y logs hasta por doce (12) meses.
- La plataforma de CyberSOC administrada deberá integrar a nivel de API un sistema de automatización de servicios profesionales TI y gestión de incidentes especializado para SOC, que le permita la documentación, diseño de procesos y automatización de la gestión de incidentes en tiempo real, la cual deberá contar mínimamente con capacidades de:
 - Transformación de alertas de seguridad y/o eventos de seguridad a tickets de forma automática.
 - Tratamiento de eventos de seguridad creando y atendiendo ticket de forma bidireccional, del Cyber SOC a la plataforma de gestión y de la plataforma de gestión al CyberSOC.
 - Definición de reglas personalizadas para dirigir tickets a equipos de trabajo específicos.
 - Creación de notificaciones automáticas cuando un evento crítico ocurre en la plataforma de CyberSOC disparando llamadas telefónicas a los recursos definidos previamente en la consola.
 - De generación de un historial de eventos y reportes detallados que podrán ser vinculados a los tickets en la plataforma de gestión de servicios profesionales especializada para CyberSOC.
 - Clasificación automática permitiendo que las alertas e incidentes de seguridad puedan tener una valoración cualitativa de al menos 4 niveles de severidad: bajo, medio, alto y crítico. Estos niveles de severidad podrán ser modificados de manera manual o automática luego en su etapa de tratamiento.



- De poder agrupar las alertas relacionadas en incidentes, así como proporcionar un contexto de este.
- De poder extraer los elementos importantes o relevantes de las alertas, y mostrarlos a manera de resumen en la pantalla de análisis del incidente.
- De contar con un dashboard donde se muestran los incidentes de seguridad que no han sido atendidos (clasificados de acuerdo con su criticidad en alta, media y baja), un resumen sobre los incidentes de seguridad (clasificados por su plataforma, etc.)
- De asignar cada alerta de seguridad a un analista administrador de la consola, esta asignación se puede hacer de forma manual o automática en base a ciertos criterios de la alerta. Por cada asignación que se realice se deberá notificar vía correo al analista.
- De asignación de estados para cada incidente de seguridad, tales como abierto, en proceso, cerrado, resuelto, o estados equivalentes.
- De colocar un comentario por cada incidente, con el objetivo de llevar un seguimiento de este durante la investigación.
- De incluir la lista de fuentes de eventos asociadas al incidente, los hosts y usuarios afectados, una matriz de MITRE ATT&CK señalando las tácticas y técnicas asociadas, el detalle de las alertas, timeline del incidente, diagrama del incidente que muestre una relación de causalidad de procesos involucrados en el incidente, WAR ROOM que permita la interacción entre los diferentes analistas que están atendiendo el incidente, la lista de playbooks seleccionados y ejecutados para resolver el incidente (así como su estado de ejecución: en proceso o finalizado), playbooks recomendados automáticamente por la plataforma, para incrementar el nivel de automatización en la resolución del incidente. Todo este detalle permitirá facilitar la labor del analista en la atención de los incidentes de seguridad.
- De poder gestionar los incidentes de seguridad detectados a partir del motor de analítica y correlación de la plataforma con IA automatizando procesos en la plataforma.
- De contar con un dashboard para monitorear el MTTR (mean time to response) en la gestión de incidentes.
- De contar con un motor automático de Scoring de incidentes, en base a determinados criterios de cada alerta de seguridad, éste deberá funcionar de manera paralela a la valoración cualitativa de los incidentes y alertas de seguridad.
- De integrar un módulo de gestión de proyectos para implementar y gestionar proyectos de remediación y mitigación de riesgos que involucren actividades como las actualizaciones de sistemas (UPGRADE), aplicación de parches de seguridad sobre activos de misión crítica, la definición de políticas de uso de software y/o aplicaciones a través de reglas, restricciones o tareas de desinstalación masivas, entre otros.
- De integrar un módulo de base de conocimiento que le permita empezar a documentar el proceso de tratamiento de eventos y artículos de interés.

5.1.1.2. CAPACIDADES DE PREVENCIÓN DE CIBERATAQUES

Se deberá ejecutar ejercicios, tres (03) ejercicios de hacking ético en modalidad de caja negra y caja gris sobre un total de ciento veinte (120) servidores, mil cuatrocientos cincuenta (1450) estaciones de trabajo, dos (02) firewalls, cuatro (04) switches



Core/Distribución, setenta (70) Routers, cuarenta (40) Switches, un (01) sistema de correo y antispam y un (01) WAF, integrando a nivel de API y correlacionado las fuentes de antivirus, EDR, XDR, antispam, correo, firewalls, switches u otros componentes de red, empleando técnicas de escaneo e intrusión para realizar el respectivo análisis de vulnerabilidades y obtener un panorama detallado de la misma, deberá evidenciarse el grado de exposición o intrusión de estos recursos ante un eventual ataque y por ende hacer las recomendaciones adecuadas del caso asistiendo de forma integral en la remediación.

Los ejercicios de hacking ético serán ejecutados bajo los siguientes lineamientos:

- OWASP (Open Web Application Security Project).
 - PTES (Penetration Testing Execution Standard).
 - OSSTMM (Open Source Security Test Methodology Manual).
 - NIST SP 800 -115 -Technical Guide to Information Security -Testing and Assessment.
 - ISSAFF (Information Systems Security Assessment Framework)
 - CVSS (Common Vulnerability Scoring System).
 - SSVC el marco de priorización de riesgos de CISA.
- Se deberán utilizar herramientas de software para determinar las posibles deficiencias de seguridad (física y lógica) que existen en los objetos de evaluación, detectándose todo tipo de vulnerabilidades, no sólo a nivel de protocolo IP sino a nivel de otros protocolos de uso común (FTP, SMTP, POP, SOCKS, etc.); además a nivel de aplicaciones y otras capas, se puede tomar como referencia el modelo OSI.
 - Los ejercicios de pentesting y hacking deberán considerar como mínimo las siguientes fases:
 - Escaneo: Analizar los sistemas con el fin de identificar puertos abiertos, aplicaciones asociadas a dichos puertos y posibles vulnerabilidades informáticas que de ser explotadas puedan constituir un riesgo para la seguridad de la información.
 - Clasificación de Riesgos: Priorización de las vulnerabilidades identificadas para su explotación tomando en consideración al menos lo siguiente: Severidad, Impacto e información que pueda ser aprovechada durante la etapa de pruebas o explotación.
 - Comprobación y/o Explotación: Ejecución de vectores de ataques previa priorización de las vulnerabilidades identificadas en base a su nivel de severidad e impacto, esto con el propósito de comprobar si la vulnerabilidad es explotable en el contexto de configuración y seguridad. Se deben excluir pruebas que pudiesen causar denegación de servicio (DoS).
 - Post – Explotación: En caso de que las pruebas de penetración sean exitosas, de acuerdo con el alcance establecido y al tiempo de ejecución, se deberá dejar evidencia o rastros de esta según corresponda, por ejemplo: Archivos de texto, Creación de usuarios, Capturas de Brechas de Seguridad, etc.
 - Generación de resultados: Se clasificará la severidad de los hallazgos de acuerdo con las mejores prácticas y se priorizará su remediación, generando como entregable un informe del servicio, con las recomendaciones para la mitigación de hallazgos identificados durante la ejecución del servicio. Dicho informe debe incluir un resumen ejecutivo y anexos técnicos detallados.
 - Se deberá tratar de obtener cuentas de usuarios (Login y Password) a través de herramientas automatizadas utilizadas por los hackers. Se utilizarán contraseñas por



defecto del sistema, diccionario de contraseñas, ataques por fuerza bruta, entre otras para determinar el respectivo grado de vulnerabilidad.

- Se deberá recopilar la mayor cantidad de información susceptible de ser utilizada para vulnerar cualquiera de las protecciones que pudiera disponer CORPAC S.A.
- Se deberá comprobar la existencia de herramientas de contención y el nivel de defensa que ofrecen frente a la llegada de código malicioso y/o ataques dirigidos.
- Se deberá realizar un diagnóstico de las vulnerabilidades a ataques de ingeniería social, ejecutando por lo menos dos (02) pruebas de ingeniería social al año, además de la propuesta adecuada para contrarrestarlos.
- Todas las actividades realizadas para el desarrollo del servicio deberán presentarse a través de la plataforma web segura que permita organizar y documentar todos los hallazgos (incluyendo evidencias) en base a la información obtenida de las pruebas, estimando el riesgo actual de las vulnerabilidades identificadas. Asimismo, se deberán evidenciar las fortalezas y debilidades de los controles de seguridad existentes.
- El servicio deberá estar orientado a la metodología a la REMEDIACIÓN DE LOS HALLAZGOS presentados por el POSTOR, por lo que La plataforma web segura deberá permitir gestionar de forma integral las actividades de remediación y documentación de cada una de las vulnerabilidades mapeadas entre los profesionales asignados por el postor (Hackers Éticos) y el equipo de sistemas de la institución.
- La plataforma web segura para la presentación de hallazgos y gestión de las remediaciones deberá generar accesos basados en roles a fin de integrar al equipo responsable en la institución, así como dejar evidencia a través de la generación de reportes y estadística en línea, a fin de que el conocimiento de los especialistas que participen en el proyecto pueda documentarse y aprovecharse como base de conocimiento para la institución corrigiendo cualquier riesgo y previniendo potenciales.
- Las plataformas web seguras deberán brindar detalle sobre las vulnerabilidades y estatus de remediación de estas durante todo el proceso lo cual implica que mínimamente se pueda:
 - Presentar la descripción de cada vulnerabilidad, con su respectivo código CVE y SSVC.
 - La asignación de nivel de gravedad (Crítica, media, baja).
 - La asignación de categoría (Configuración, desarrollo, obsolescencia, sistema, servidor, usuario).
 - El relacionamiento con activos específicos tratados.
 - El relacionamiento con otras vulnerabilidades y actividades específicas realizadas para la mitigación en caso de no poder remediarse.
 - El detalle de la solución con información adicional de referencia y carga de evidencia como captura de pantallas.
 - El detalle de requerimiento consulta y actividades de los usuarios y su relación con el proyecto (Informador, resolutor o auditor).
 - La documentación histórica de consultas de los usuarios responsables de la remediación con asistencia cronológica.
 - La carga de evidencia que valide la corrección aplicada por ende la certificación de la remediación.
 - El informe de re-testing con imagen de evidencia.
 - Las recomendaciones y consideraciones de seguridad de la red interna.
 - El detalle de cierre del caso para posterior certificación por parte del equipo de la institución.



- La información estadística con los hallazgos y remediaciones del primer test Vs la segunda prueba.
- Gráficos estadísticos que ayuden a evidenciar de manera práctica y objetiva vulnerabilidades reportadas, vulnerabilidades corregidas y vulnerabilidades aun latentes o abiertas.
- El acceso a la plataforma deberá estar vigente por mil noventa y cinco (1095) días calendarios, manteniendo un acompañamiento proactivo evaluando vulnerabilidades y riesgos potenciales, habilitando consultas y respuestas a los especialistas (hackers éticos) a través de la plataforma web segura recibiendo la asesoría integral sobre las remediaciones recomendadas y su impacto sobre los servicios.
- El servicio debe incluir la suscripción de una plataforma destinada a la reducción de superficie de ataque externa, a través del descubrimiento y explotación continua de vulnerabilidades y pentesting sobre los activos de misión crítica de CORPAC S.A. permitiendo mínimamente:
- Que se integre a nivel de API a la consola de administración SOAR o CyberSOC administrado responsable de orquestar las capacidades de correlación, detección y respuesta.
- Que permita la automatización de las pruebas de penetración e identificación de riesgos sobre los activos publicados.
- Que este desarrollada sobre un marco de mejora continua el tiempo, brindando detalles de las remediaciones a aplicar por cada vulnerabilidad o riesgo asociado al activo.
- Que realice automáticamente el filtrado de salida para garantizar que la organización esté restringiendo efectivamente el tráfico de salida innecesario, evitando de esta manera que un determinado acceso pueda permitir que un actor malicioso exfiltre datos del sistema de la organización.
- Que audite la autenticación ataques al descubrir la cuenta de usuario credenciales, fin de que automáticamente se intente validar esas credenciales y determinar dónde son más útiles. Este es un proceso común ejecutado por atacantes maliciosos y probadores de penetración y realizado durante la escalada de privilegio por lo que es de vital importancia que la plataforma sea la primera en ejecutar la validación.
- Que audite y valide la escalada de privilegios y movimiento lateral usando un conjunto válido de credenciales identificando áreas valiosas dentro de su organización. Esto es llevado a cabo a través de una variedad de métodos y herramientas a fin de poder ejecutar netstat de forma recursiva en múltiples hosts, proporcionando salida y representación visual del flujo de datos (o conexiones de red) dentro del entorno.
- Que pueda detectar y documentar la exfiltración de datos a través de la simulación y registro de esta actividad para ayudar al equipo de informática de la ENTIDAD para ajustar configuraciones y cerrar brechas de seguridad.
- Que pueda hacer uso de acceso elevado e intentar cargar código malicioso en sistemas remotos en un intento de probar la protección de punto final de la organización a fin de afinar los controles antimalware.
- Que pueda generar un informe ejecutivo y un informe técnico acerca de una vulnerabilidad y automatizar la prueba de penetración documentando la capacidad de respuesta que se tuvo frente a esta.
- Que pueda configurarse para analizar objetivos externos publicados a internet u objetivos internos como servidores y/o aplicaciones.
- Que pueda presentar informes de penetración y remediación de forma trimestral evidenciando la evolución de los ejercicios.
- Que permita la creación automática de un ticket con la identificación de vulnerabilidad o éxito de ejercicio de penetración.
- El servicio debe incluir la suscripción de una plataforma destinada a la reducción de superficie de ataque interna, a través del descubrimiento y priorización de vulnerabilidades de forma continua, teniendo por objetivo la remediación y mitigación



efectiva del riesgo en el tiempo sobre la totalidad de los servidores de CORPAC S.A. permitiendo mínimamente:

- La presentación sea de tipo SaaS con una arquitectura basada en agente ligero el cual no supere los 20 MB de tamaño para su óptimo desempeño.
- Que permita implementar una gestión avanzada de vulnerabilidades, configuraciones alineadas a cumplimiento normativo como ISO y NIST.
- Que permita optimizar el proceso de priorización de riesgos utilizando una metodología de priorización de riesgos SSVC la cual consiste en un sistema que ayuda a analizar las vulnerabilidades para tomar decisiones que contribuyan a prevenir incidentes de seguridad y contener sus consecuencias.
- Que permita tratar las vulnerabilidades según su nivel de explotabilidad mínimamente con los siguientes criterios: fácilmente explotable, explotable en la red, explotación pública disponible, explotación con alto movimiento lateral.
- Que tenga la capacidad de relacionar las vulnerabilidades con ataques de alta fidelidad, las vulnerabilidades de los kits de explotación que se pueden utilizar para explotar la debilidad. Esto debe permitir predecir un ataque específico arrojando las coordenadas exactas para mitigarlo.
- Mantener activo el proceso de descubrimiento de activos de TI de forma automática y permitir generar alertas de uso indebido de aplicaciones o software a los responsables.
- Gestionar de forma integral la corrección de errores de configuración y controles de seguridad para fortalecer los sistemas.
- Gestionar procesos de remediación y/o mitigación de riesgos basados en la identificación, clasificación y distribución efectiva de parches de actualización para mitigar los riesgos de seguridad considerando parches sobre Windows, Linux, macOS y todas las aplicaciones instaladas sobre los hosts tales como navegadores, bases de datos, componentes, etc.
- Evaluar el cumplimiento normativo mínimamente de NIST CSF e ISO a través de la validación que realice el agente instalado sobre los hosts seleccionados cubriendo mínimamente la siguiente lista de puntos de referencia:
 - Tiempo mínimo de la contraseña.
 - Permitir estados de espera cuando el equipo o servidor inicio sesión.
 - Requerir una contraseña cuando una computadora se activa.
 - Criptografía del sistema para el forzado de una fuerte protección de claves para las claves de usuario almacenadas en la computadora.
 - La clave debe cumplir los requerimientos de complejidad.
 - Desactivar la prevención de ejecución de datos para el ejecutable de ayuda HTML.
 - Requerir contraseña al conectarse.
 - Habilitar la autenticación del cliente del asignador de extremos de RPC.
 - Requerir autenticación de usuario para conexiones remotas mediante autenticación de nivel de red.
 - Requerir el uso de inicio rápido.
 - Desactivar la prevención de ejecución de datos para Explorer.
 - Hacer cumplir el historial de contraseñas.
 - Seguridad de la red: nivel de autenticación de LAN Manager.
 - Control del comportamiento del Registro de eventos cuando el archivo de registro alcanza su tamaño máximo (Seguridad).
 - Inicio de sesión interactivo: límite de inactividad de la máquina.
 - Desactiva las notificaciones de aplicaciones en la pantalla de bloqueo.
 - Permitir el acceso remoto a la interfaz Plug and Play.
 - No procesar la lista de ejecutar una vez para la configuración del equipo.
 - No enumerar usuarios conectados en equipos unidos a un dominio.



- Umbral de bloqueo de cuenta.
 - Seguridad de red: seguridad de sesión mínima para clientes basados en NTLM SSP (incluido RPC seguro).
 - Acceso a la red: no permitir la enumeración anónima de cuentas y recursos compartidos SAM.
 - No procesar la lista de ejecución heredada para la configuración del equipo.
 - Impedir la instalación de dispositivos extraíbles.
 - Longitud mínima de la contraseña.
 - Criptografía del sistema: use algoritmos compatibles con FIPS para el cifrado, el hash y la firma.
 - Control de cuentas de usuario: eleve solo las aplicaciones de UIAccess que están instaladas en ubicaciones seguras.
 - Acceso a la red: rutas y subrutas de registro accesibles de forma remota.
 - Miembro del dominio: cifre o firme digitalmente los datos del canal seguro (siempre).
 - Control de cuentas de usuario: Comportamiento del aviso de elevación para usuarios estándar.
 - Control de cuentas de usuario: detecte instalaciones de aplicaciones y solicite la elevación.
 - Cuentas: estado de la cuenta de invitado
 - Acceso a la red: restrinja el acceso anónimo a canalizaciones con nombre y recursos compartidos.
 - Acceso a la red: no permitir la enumeración anónima de cuentas SAM.
 - Acceso a la red: permite que los permisos de Todos se apliquen a usuarios anónimos.
 - Control de cuentas de usuario: ejecute todos los administradores en modo de aprobación de administrador.
 - Control de cuentas de usuario: eleve solo los ejecutables que estén firmados y validados.
- Consolidar y presentar el análisis y búsqueda de vulnerabilidades, configuraciones erróneas alineadas a cumplimiento NIST, anomalías de postura que deriven del uso de procesador, red, memoria, puertos, servicios, usuarios, perfiles, etc. y otros riesgos de seguridad.
 - Ejecutar acciones para alinear políticas de uso de los activos tales como:
 - Bloquear una aplicación por determinado tiempo.
 - Permitir la ejecución de aplicaciones en determinados intervalos de tiempo.
 - Bloquear y determinar el acceso a dispositivos por determinado intervalo de tiempo.
 - Enviar un script.
 - Gestionar un proceso.
 - Gestionar el status de un servicio.
 - Gestionar un registro.
 - Instalar o desinstalar una aplicación por determinados periodos de tiempo.
 - Evaluar la actividad de la red.
 - Evaluar la transferencia de archivos.
 - Validar que programas inician sesión.
 - Borrar un archivo.
 - Mover un archivo a cuarentena.
 - Modelar la creación de informes completamente personalizables y listos para auditorías, presentando mínimamente informe de inventario o exposición de activos, informes de incumplimiento de políticas de uso de software, informes de vulnerabilidades con su respectivo nivel de riesgo basado en múltiples criterios, informes de aplicación de parches sobre sistemas operativos y aplicaciones instaladas,



informes de anomalías con indicadores de ataque (IoA) e indicadores de compromiso (IoC) e informes de cumplimiento de la NIST y/o ISO, evidenciando la reducción del riesgo en el tiempo.

- El servicio debe incluir la suscripción activa de una plataforma de Cyber Threat Intelligence con capacidad de detectar y disuadir amenazas externas a partir de una investigación profunda y continua de la dark web y otros canales de comunicación utilizados por los cibercriminales, cumpliendo mínimamente con los siguientes requisitos:
- Deberá ser presentada en modalidad de Security as a Service (SECaaS) delegando toda la responsabilidad de investigación, síntesis y presentación de evidencia objetiva de amenazas.
- Deberá poder integrarse a nivel de API con una plataforma SOAR o CyberSOC administrado a fin de ingerir automáticamente la inteligencia generada, disparar alertas automáticas y generar tickets en el momento que se realice un incidente.
- Deberá poder activar para la suscripción el módulo de credenciales y el de hacktivismo por el período de suscripción del contrato.
- Deberá detectar credenciales comprometidas de institución, las credenciales que se recuperan pueden estar relacionadas con clientes externos, afiliados de terceros y aplicaciones comerciales y de TI internas.
- Deberá reconocer robo de credenciales de botnets las cuales han sido robadas por los servidores de crime logrando determinar el origen de la fuente, ya sea por configuraciones incorrectas y/o robo a través de herramientas de malware identificando el nombre de la botnet responsable y técnicas de ingeniería social utilizadas.
- Deberá reconocer credenciales de hacktivismo las cuales han sido filtradas en fuentes de cibercrimen y hacktivistas como foros, sitios de pegado, P2P, sitios web oscuros, etc.
- Deberá monitorear la actividad de hacktivismo en redes sociales, sitios de pegado, chats IRC, etc. para saber si existen grupos de hacktivismo que buscan atacar activos tecnológicos de la institución.
- Deberá permitir identificar y detectar vulnerabilidades y ataques desde el día 0, que afectan el software y hardware utilizado por la institución.
- Deberá integrar capacidades de predictibilidad basada en la recopilación de datos de fuentes abiertas, cerradas y privadas a través del 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 foros, FTP servers, Marketplaces y otros lugares no divulgados) para encontrar indicios o evidencias de amenazas existentes o emergentes que puedan atentar contra la INSTITUCIÓN.
- Deberá presentar detalles de los hallazgos del módulo de credenciales, entregando mínimamente los siguientes datos:
 - Posibilidad de categorizar el nivel de criticidad y/o prioridad de las credenciales encontradas.
 - Usuario y contraseña comprometida.
 - Tipo de botnet relacionada
 - URL afectada y/o plataforma o servicio afectado
 - Palabras clave utilizadas para la captura
 - Tipo de credencial
 - Clasificación
 - Relación con plataforma de correo
 - Última actualización
 - Fecha de reporte
 - Fecha de violación o captura



- Deberá presentar detalles de los hallazgos del módulo de hacktivismo, entregando mínimamente los siguientes datos:
 - Título
 - Palabras relacionadas
 - Idioma
 - País
 - Relevancia
 - Origen
 - Tipo
 - URL y/o activo afectado
 - Fecha de reporte
 - Fecha de última actualización
- Deberá permitir la creación de alertas para todos sus módulos.
- Deberá poder afinar la búsqueda a través de filtros, parámetros y clasificación por dominio, IP o palabra para todos sus módulos.
- Deberá poder integrar datos de amenazas STIX/TAXII e intercambio de información con el SIEM o SOAR o Plataforma de CyberSOC administrada que la institución implemente.
- Deberá documentar más de 10 años de datos históricos sobre amenazas, esto confirma el nivel de conocimiento de se tiene de redes ciberterroristas y actores maliciosos.
- Deberá presentar complementos disponibles para SIEM, SOAR y TIP y/o Plataformas de CyberSOC Administradas.
- Deberá administrar un sistema dinámico de puntuación de riesgos para alimentar programas de gestión de vulnerabilidades a través de API.
- Deberá integrar puntuación y clasificación de amenazas de malware.
- Deberá integrar en sus procesos la entrega verificada por humanos a fin de minimizar falsos positivos.
- Deberá integrar una asociación continua con Cyber Threat Alliance (CTA).
- Deberá de tener una arquitectura modular que permita activar diferentes funcionalidades en el tiempo, estas funcionalidades deberán comprender mínimamente el compromiso de credenciales, protección de dominio, fuga de datos, hacktivismo, tarjetas de crédito, monitoreo de la organización en la dark web, exploración de amenazas, monitoreo de la organización en redes sociales e indicadores de ataque.

5.1.1.3. CAPACIDADES DE DETECCIÓN Y RESPUESTA EFECTIVA ANTE CIBERATAQUES

- La plataforma de CyberSOC administrada deberá monitorear, correlacionar, detectar y responder ante cualesquiera incidentes y/o eventos de seguridad de forma autónoma, visando y notificando el tratamiento de cada evento por el equipo de analistas del fabricante de la plataforma, cubriendo un monitoreo efectivo las 24 horas del día los 7 días de la semana.
 - La plataforma de CyberSOC administrada deberá estar integrada a nivel de API con:
 - La plataforma de reducción de superficie de ataque (Vulnerabilidades y pentesting).
 - La plataforma de Cyber Threat Intelligence (Monitoreo efectivo en dark web).
 - La solución antivirus con la que cuente la institución.
 - La solución EDR / XDR con la que cuente la institución.
 - La solución de firewall con la que cuente la institución.
 - La plataforma de correo con la que cuente la institución.
 - La plataforma avanzada de gestión de incidentes para CyberSOC.
- Esto a fin de optimizar los tiempos de respuesta a través de la construcción de procesos específicamente diseñados para la institución.
- La plataforma de CyberSOC administrada debe integrar capacidades de detección avanzada de infracciones reconociendo tácticas, técnicas y procedimientos (TTP) del



adversario de acuerdo con el marco MITRE ATT&CK presentando capacidades efectivas de MDR.

- La plataforma de CyberSOC administrada deberá estar diseñada para buscar TTP sobre el dispositivo local Windows, Mac y Linux en varias categorías, incluidas mínimamente descubrimiento, persistencia, evasión de defensa, ejecución, acceso a credenciales, escalada de privilegios y movimiento lateral.
- La plataforma de CyberSOC administrada deben incluir funciones de búsqueda a través de sistemas de cacería de amenazas avanzadas y feeds de búsqueda de inteligencia de amenazas automatizadas considerando mínimamente las siguientes metodologías de prueba de búsqueda de amenazas como Browser visit, DNS Cache Entry, Driver File Hash, Driver File Name, File Hash, File Name, Event in log source, Event in log category, Event ID in log, Event type in log, Service state, User Account, Network connection, Process Hash, Process Name, Registry Key y YARA rules.
- La plataforma de CyberSOC administrada deberá detectar la actividad de minería de criptomonedas de los mineros de criptomonedas basados en el navegador, así como del software cliente de minería de criptomonedas comúnmente conocido que reside en el dispositivo local mapeando toda la actividad relacionada.
- La plataforma de CyberSOC administrada deberá mapear conexiones de red entrantes y salientes las cuales deberán ser registradas y analizadas para detectar amenazas en la red. La actividad maliciosa se identificará evaluando el puerto utilizado, la reputación y la geolocalización de la dirección IP y otras atribuciones disponibles.
- La plataforma de CyberSOC administrada deberá detectar ransomware verificando el sistema local en busca de actividades de cifrado permitiendo a los usuarios eliminar el proceso infractor o aislar el host afectado automáticamente, deteniendo los ataques de ransomware inmediatamente después de la detección.
- La plataforma de CyberSOC administrada deberá contar con un monitor de registro de eventos de punto final logrando ingerir los eventos relacionados con la seguridad escritos en el registro de eventos pudiendo agregar identificadores de eventos personalizados para monitorear aplicaciones personalizadas.
- La plataforma de CyberSOC administrada deberá contar con la capacidad de analizar registros de firewall enviando datos a Data Center SOC a través de Syslog para monitorear los eventos de seguridad registrados y tener la posibilidad de integración a nivel de API.
- La plataforma de CyberSOC administrada debe integrar capacidades de detección de indicadores de compromiso (IoC), esta aplicación deberá ejecutar detecciones seleccionadas por el equipo del Data Center CyberSOC a través de su equipo de investigación de amenazas y se puede actualizar según sea necesario sin que el administrador o el usuario deban realizar ninguna acción.
- La plataforma de CyberSOC administrada debe presentar un entorno de trabajo colaborativo evidenciando los diferentes eventos de detección basados en múltiples fuentes de información sobre amenazas. El Data Center SOC supervisará estas detecciones y las tratará con alta prioridad, y el equipo de investigación de amenazas seguirá supervisando las métricas de detección para ajustar los falsos positivos o los falsos negativos.
- La plataforma de CyberSOC administrada debe contar con la capacidad de detectar archivos maliciosos a través de su propio motor de detección de malware desarrollado como parte de la solución integrada, escaneando archivos escritos en el disco o ejecutados en busca de atributos maliciosos para proporcionar redundancia sobre la solución antimalware con la que ya cuenta la institución.
- La plataforma de CyberSOC administrada debe contar con la capacidad de detectar servicios de red sospechosos que se ejecutan en servidores y estaciones de trabajo. Si bien existen múltiples servicios de red disponibles para uso legítimo, las detecciones



sospechosas se definen como puertos y servicios conocidos que se aprovechan con fines maliciosos por lo que es de vital importancia la evaluación de cada uno de estos servicios.

- La plataforma de CyberSOC administrada debe contar con la posibilidad de detectar herramientas sospechosas y/o programas que puedan afectar negativamente la seguridad del sistema y la red. Las herramientas sospechosas detectadas deben investigarse y clasificarse como utilidades de piratería, descifradores de contraseñas u otras herramientas utilizadas por atacantes con fines maliciosos.
- La plataforma de CyberSOC administrada debe poder configurarse para habilitar la monitorización de registros de unidades USB (Medios extraíbles) para mapear cuando un dispositivo USB se conecta y se desconecta.
- La plataforma de CyberSOC administrada debe contar con capacidades de respuesta ante ataques en curso, aislando dispositivos en la red que tengan instalado un agente, el aislamiento del host se realizará como consecuencia de un análisis y/o activación automática de un playbook de respuesta a incidentes para evitar la propagación de código malicioso al impedir que una máquina vulnerada se comuniquen con otros dispositivos de red en internet o la red del cliente. La máquina aislada mantendrá la conectividad con la plataforma correspondiente y permitirá que el Data Center SOC o equipo responsable en la institución reconecten el dispositivo.
- La plataforma de CyberSOC administrada debe contar con capacidades de respuesta y remediación a través del agente, logrando ejecutar la eliminación de archivos, eliminación de claves y valores del registro, terminación de procesos, desinstalación de software, parada de servicios, eliminación de tareas programadas.
- La plataforma de CyberSOC administrada deberá mostrar mínimamente:
- Por cada activo protegido el detalle de las potenciales brechas de seguridad en función a la cantidad de eventos maliciosos y eventos sospechosos especificando la telemetría y detalle de cada evento analizado.
- Por cada activo protegido todos los eventos detectados en orden cronológico permitiendo visualizar objetivos, tácticas y técnicas previstas por los atacantes ayudando a interrumpir rápidamente un proceso de ataque reduciendo el tiempo de permanencia, cada evento en el tiempo deberá de mostrar la fecha y hora exacta de la detección, la IP local, el puerto, IP remota el puerto remoto el país y el detalle de la conexión o telemetría del evento.
- Por cada activo protegido información detallada del servidor y/o estación custodiada en línea con información detallada del inventario del activo permitiendo conocer: Configuración del sistema y configuración de red, Detalle de los servicios (Nombre, tipo, estado y ubicación), Software instalado (Fabricante, usuario, versión, tamaño y fecha de instalación), Usuarios y sesiones activas, Status de aplicación de políticas de contraseñas, Recursos compartidos, Estado de la red (Netstat) y tabla ARP, Status de Update y Upgrade.
- La plataforma de CyberSOC administrada deberá informar sobre los datos de registro de Microsoft Office 365, Azure y Microsoft Exchange integrándose al tenant de Microsoft Office 365 de cuentas activas y funcionar en modalidad de Security as a Service sin demandar la instalación de ningún componente adicional y tercerizando la gestión de ciberseguridad con el fabricante agregando mínimamente las siguientes capacidades:
- Ejecución de monitoreo activo y efectivo con correlación, evaluación, detección y respuesta las 24 horas del día los 7 días de la semana.
- Habilitación en modalidad de seguridad con administración delegada al fabricante.
- Proporcionar una alerta temprana de actores malintencionados sobre Microsoft 365.
- Alerta sobre los intentos de crear nuevas cuentas, acceder a las cuentas existentes o aumentar los permisos de las cuentas existentes, detectando mínimamente, inicios de sesión fuera de los países esperados o direcciones IP maliciosas conocidas e intentos de Inicio de sesión.



- Ejecución de una rutina inusual o no reportada las misma que deberá ejecutar automáticamente la creación de un ticket y a la vez la generación de una llamada telefónica que notifique y exponga el intento de ataque o violación de seguridad en el momento que ocurra.
- Evaluación continuamente de los riesgos en usuarios, las aplicaciones y el inicio de sesión en función de la heurística y el aprendizaje automático para identificar comportamientos que pueden representar una amenaza para la institución o presencia en línea.
- Identificación y mitigación de amenazas relacionadas con accesos no autorizados, accesos desde ubicaciones inusuales y dispositivos desconocidos.
- Análisis de patrones de inicio de sesión para detectar anomalías.
- Generación de alertas de seguridad para respuesta inmediata.
- Correlación de eventos de autenticación con indicadores de amenazas permitiendo la integración con sistemas de respuesta automatizada.
- Supervisión de eventos y registros de seguridad en Office 365 extrayendo información de Microsoft Graph, que tiene acceso a los datos de todos los productos habilitados para la nube de Microsoft.
- Auditoria de cambios en configuraciones de seguridad.
- Generación de informes detallados de actividad sospechosa y evaluar reglas de redireccionamiento de correos.
- Presentación de eventos con telemetría en sus reportes: Veredicto, Fecha y hora de detección, User de correo, Localización, Reputación, Resultado, Detalle de la amenaza.
- Acción automática en caso de detectar un inicio sospechoso de sesión exitoso de O365, se deberán analizar los detalles (EMAIL y PROCEDENCIA) y se deberá escribir el evento en una línea de tiempo a fin de sustentar la implementación de estrategias de mitigación.
- Detección de riesgos sobre unlikelyTravel, passwordSpray, leakedCredentials, impossibleTravel.
- Archivar los eventos de acuerdo con el tratamiento y/o políticas que se apliquen sobre estos.
- Enfocar el análisis en las cuentas, los usuarios y los comportamientos más riesgosos. Riesgo determinado a través de una combinación de heurística de la industria y aprendizaje automático.
- Presentación de descripción general de la postura de seguridad en la nube con planes de corrección detallados en todos los inquilinos de Office365 y/o Microsoft Exchange.
- La plataforma de CyberSOC administrada deberá considerar la detección de eventos considerados como amenazas, que tengan un potencial de causar daño o impacto. Los eventos incluyen el acceso no autorizado a las computadoras, el uso no autorizado de los privilegios del sistema y la ejecución de malware que destruye, cifra un sistema o roba datos. Teniendo en cuenta que:
- Un evento se considera como una ocurrencia observable, como cuando se produce un inicio de sesión fallido en una computadora. Si bien esto podría ser intencional o no intencional, ambos se consideran eventos.
- Un incidente de seguridad es una violación o amenaza inminente de las políticas de seguridad o las mejores prácticas de la industria.
- La plataforma de CyberSOC administrada deberá poder detectar eventos relacionados mínimamente a: Denegación de servicio, Phishing, Malware, Ransomware, Secuestro de RDP, PowerShell, Compromiso de EMAIL (Business Email Compromise - BEC), Ataque de intermediario (Man-in-the-middle attack - MITM), Explotación de día cero, Cryptojacking (minería de criptomonedas maliciosa), Túnel DNS, Ataque Drive-by y Ataque de espionaje.
- La plataforma de CyberSOC administrada debe ser capaz de recopilar mínimamente registros específicos del sistema operativo y de seguridad los cuales enviará al CyberSOC o centro de control para detectar eventos de seguridad, proporcionar datos a



los analistas del CyberSOC para clasificar los incidentes y almacenar registros con fines de auditoría histórica.

- La plataforma de CyberSOC administrada deberá poder registrar mínimamente los siguientes eventos de acuerdo a las plataformas protegidas, Para Sistemas Operativos Windows: 104 Se borró el registro de seguridad del sistema, 1102 Security - Se borró el registro de auditoría, 4722 - Security - Se habilitó una cuenta de usuario, 4735 - Security - Grupo local cambiado, 7040 - System - El servicio se cambió de inicio automático a deshabilitado, 7034 - System - Servicios terminados inesperadamente, 4702 - Security - Se modificó una tarea programada, 5142 - Security - Se agregó un objeto de recurso compartido de red, 5144 - Security - Se eliminó un objeto de recurso compartido de red, 4625 - Security - Una cuenta no pudo iniciar sesión, 7036 - System - Un servicio defensivo fue detenido, 5145 - Security - Se ha comprobado un objeto de recurso compartido de red por PsExec, 4649 - Security - Se detectó un ataque de repetición, 64004- System - Protección de archivos de Windows no pudo restaurar el archivo a su versión original, 5143 - Security - Se modificó un objeto de recurso compartido de red, 4740 - Security - Se bloqueó una cuenta de usuario, 4698 - Security - Se ha creado una nueva tarea programada, 7031 - System - El servicio finalizó inesperadamente, 4738 - Security - Se ha cambiado la contraseña de la cuenta de usuario, 4724 - Security - Se ha intentado restablecer la contraseña de una cuenta, 4720 - Security - Cuenta de usuario de prueba creada y 1100 - System - Se cerró el registro de eventos.
- Para sistemas operativos Mac: Log Privacy - Privatizar el contenido de registro que contiene nombres de usuario, direcciones IP y otra información confidencial, Watch_Logon - Inicios de sesión de usuario en el sistema, SSH_connection - Conexiones SSH entrantes a la Mac, Watch_Logout Cierres de sesión del usuario del Sistema, Failed_Auth - Error de autenticación de usuario, Sudo_Usage - Escalada de privilegios usando sudo.
- Para sistemas operativo Linux: Sudo_Usage - Escalada de privilegios usando sudo, SSH_login - Conexiones SSH entrantes a la Mac, SSH_failed login - Error en los inicios de sesión SSH entrantes, User_add - Se ha creado una nueva cuenta de usuario, Password_change - Se ha cambiado la contraseña de un usuario, Group_change - Se cambió un grupo, Del_user_group - Se ha quitado un usuario de un grupo, Failed_Auth - Error de autenticación de usuario, SSH_login_pkey - Se detectó correctamente el inicio de sesión de clave pública a través de SSH, SSH_login_pkey_failed - Error al iniciar sesión con clave pública a través de SSH, user_del - Se ha eliminado una cuenta de usuario, new_group - Se creó un nuevo grupo, add_user_group - Se agregó un usuario a un grupo.
- Se deberá considerar la integración de una plataforma de seguridad tipo WAF y/o WAAP para los servicios críticos que se publican en la institución, garantizando que esta mínimamente pueda:
- Detectar ataques tipos xxs, xsx, csrf, campos ocultos, envenenamiento de cookies, inyecciones de código, inyecciones sql, alteración de parámetros, backdoors, stealth commanding, navegación forzada, vulnerabilidades conocidas, exploits conocidos, top ten OWASP y de día cero.
- Analizar comunicaciones http y https.
- Cumplir con estándares PCI DSS.
- Detección en función a reglas, sintaxis, firmas actualizadas por servicio en la nube, patrones e inteligencia artificial.
- Modelo de seguridad mixto positivo – negativo.
- Administración basada en Nube.
- Monitoreo basado en Nube e integración con otros sistemas de monitoreo como SYSLOG y SIEM.
- La plataforma de CyberSOC administrada deberá integrar un sistema de gestión de acceso, identidad segura (IAM) y gestión de privilegios que garantice que los usuarios



permitidos tengan el acceso adecuado a los recursos adecuados, todo desde los dispositivos adecuados y las ubicaciones aprobadas, solicitando mínimamente que:

- El sistema tenga integración nativa con la plataforma de CyberSOC administrada propuesta.
- El sistema combine autenticación de dos factores (2FA), inicio de sesión único (SSO) y administración de contraseñas (PM) junto al monitoreo continuo de la dark web para detectar si las credenciales del usuario han sido comprometidas y expuestas en la dark web.
- Que se permita que los técnicos reserven usuarios en cuentas compartidas para proteger cuentas privilegiadas con 2FA
- Que se acceda a una biblioteca de aplicaciones para el inicio de sesión único (SSO) o se configure una específica para CORPAC S.A.
- Que se acceda fácilmente a todas las aplicaciones desde su Launchpad.
- Que sea compatible con SAML, OpenID Connect y OAuth 2.0.
- Que se protejan las credenciales compartidas dentro de las bóvedas de contraseñas
- Que se gestione el acceso a las credenciales solo a aquellos usuarios que deberían tenerlas.
- Que se registren todas las visualizaciones de contraseñas.
- Que se almacene de forma segura todo tipo de contraseñas para máquinas, redes, aplicaciones y sitios web.
- Que se rote automáticamente las contraseñas cuando se visualizan para cuentas de Windows y Active Directory.

5.1.1.4 CAPACIDAD DE PREVENIR LA FUGA DE INFORMACIÓN

- La solución deberá incluir un componente web en modalidad SaaS que le permita extender el perímetro de seguridad de la información a documentos Microsoft Office, imágenes y PDF, logrando garantizar la privacidad, confidencialidad e integridad de la información.
- La solución deberá tener control sobre la información que se comparte fuera de la institución.
- La solución deberá garantizar el acceso seguro a la consola de administración a través de la habilitación de validación 2FA.
- La solución deberá poder determinar que un usuario receptor o propietario de la información solicite acceso bajo demanda a determinada información.
- La solución deberá permitir que se protejan documentos confidenciales a través de la instalación de un agente responsable de cargar la identidad del propietario y/o receptor.
- La solución deberá permitir que se comparta de manera controlada y segura información entre personal interno y con otras instituciones además de proteger el intercambio de información con proveedores de servicio.
- La solución deberá poder gestionar múltiples dominios.
- La solución no dependerá de licenciamiento Microsoft adicional para funcionar con normalidad.
- La solución deberá poder trabajar en modo SaaS permitiendo la protección (cifrado) de ilimitados documentos, con posibilidad de asignar privilegios de lectura, lectura y escritura o lectura, escritura y control total, a diferentes usuarios dentro y fuera de la red.
- La solución deberá integrar capacidad de gestión avanzada tales como:
- Monitorización en tiempo real lo que pasa con los documentos compartidos, IP de acceso, privilegios utilizados y usuarios que tuvieron acceso al documento.
- Reasignación de privilegios o destruir el documento en remoto en el momento que mejor convenga.
- Protección de carpetas de forma automática e integrarse al directorio activo.
- Configuración de marcas de agua dinámicas en los documentos PDF e imágenes.
- Límite del acceso a un determinado número de dispositivos logrando especificar si solo se permitirá el acceso desde un solo dispositivo o más.
- Seguimiento y monitorización de los documentos protegidos a través de los eventos de acceso.



- Utilización de un componente web que le permita el acceso a un documento sin instalar ningún tipo de agente o plugin en el equipo del receptor.
- Creación de políticas de seguridad se asocie a grupos de usuarios y perfiles de acceso específico.
- Otorgamiento de permisos completos a administradores al abrir archivos incluso si no se otorgaron explícitamente.
- Configuración para forzar en el cliente el borrado del archivo original una vez protegido (Cifrado).
- Forzado del tipo de inicio de sesión del usuario.
- La asistencia de un proceso de clasificación a nivel de la información a nivel de metadatos, pudiendo determinar sobre la información tipos de clasificación como secreto, reservado, confidencial y difusión limitada.
- Habilidad desde la consola central la función de clasificación de la información.
- La solución deberá poder generar informes usuarios internos, usuarios externos, documentos internos, documentos externos, documentos eliminados e informe de actividad permitiendo aplicar filtros sobre la búsqueda.
- La solución deberá poder configurar marca blanca sobre la plataforma.
- La solución deberá poder personalizar mensajes de sello de agua para los documentos confidenciales.
- La solución deberá poder considerar un módulo de clasificación de documentos.

5.1.1.5 EVALUACIÓN DE LAS DEFICIENCIAS EN MATERIA DE CIBERSEGURIDAD Y EJECUCIÓN DE PLAN DE TRATAMIENTO CON MEJORA CONTINUA DE NIVELES DE MADUREZ

- Se deberá incluir un servicio para definir el proceso y las actividades necesarias para lograr un nivel aceptable de seguridad y riesgos, para mejorar la postura de seguridad de la organización mediante la implementación del estándar ISO 27001:2022 / NISTIR 8374.
- Se deberá llevar a cabo mediante un proceso continuo de evaluación, seguimiento y mejora de la seguridad de la información, asegurando el cumplimiento de los controles y mejores prácticas establecidos por framework de la NIST.
- El servicio deberá abarcar:
- La evaluación inicial del nivel de cumplimiento de los controles de seguridad existentes dentro de la organización, conforme a los requisitos establecidos la NIST.
- La evaluación de los activos según el alcance definido por la organización, con sus respectivos controles de acuerdo con la NIST.
- Definir y recomendar un plan de acción basado en los controles de seguridad establecidos, según el alcance definido, para alcanzar progresivamente un nivel aceptable de protección frente a los riesgos, garantizando el cumplimiento de los requisitos de la NIST.
- Integración de los principios de mejora continua que faciliten el crecimiento y fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI), asegurando una evolución constante hacia un nivel aceptable y cumplimiento conforme a los estándares de la NIST.
- Se deberá realizar el diagnóstico inicial:
- Recopilación de información a través de entrevistas con personal clave.
- Evaluación preliminar del estado de los procesos y controles de seguridad de la información.
- Identificación inicial de brechas en relación con la NIST.
- Se deberá realizar el análisis de cumplimiento
- Revisión exhaustiva de la documentación disponible, incluyendo políticas, procedimientos y registros relevantes.
- Evaluación del grado de cumplimiento con los requisitos de la norma.
- Identificación de los controles que requiere los riesgos encontrados.
- Se deberá realizar el análisis de activos según el alcance:
- Identificación y valoración de los activos representes de acuerdo con el alcance definido por la organización.
- Identificación de las amenazas y vulnerabilidades en los activos.



- Descripción del riesgo de seguridad de la información.
- Evaluación del riesgo de los activos existentes en el proceso de la organización.
- Identificación de los controles de acuerdo con el resultado de la evaluación del riesgo de los activos.
- Se deberá presentar los siguientes entregables:
- Informe detallado que incluye: Análisis de cumplimiento, Análisis de activos, controles, recomendaciones específicas para mitigar riesgos y mejorar la conformidad.
- Excel de los resultados obtenidos en el servicio.
- Presentación ejecutiva de los resultados.
- Como parte del servicio, el diagnóstico inicial, se deberá desarrollar los primeros treinta (30) días calendarios una vez iniciada el servicio. El análisis de cumplimiento, en 30 días calendarios una vez iniciada la etapa de operación del servicio, esto puede variar dependiendo de la rapidez con la que CORPAC S.A. proporcione la documentación solicitada.
- El servicio deberá considerar el acompañamiento continuo del proceso de mejora continua, definiendo objetivos semestrales, presentando informes que evidencien el alineamiento progresivo con los principios de la NIST.
- El CONTRATISTA debe proveer un sistema de gestión de servicios profesionales o gestión de incidencias el cual se integrará nativamente con la plataforma de CyberSOC administrada propuesta, registrando todos los incidentes de forma automática y bidireccional.

FORMACIÓN AVANZADA PARA LOS INTEGRANTES DEL PROYECTO

- Se deberá considerar un taller y/o curso oficial de especialización en ciberseguridad dirigido a cinco (05) Profesionales Informáticos como responsables dentro de la corporación, este deberá preparar e incluir un proceso de certificación internacional de tipo Cybersecurity Certified Expert (CSCE) o CSX Cybersecurity Practitioner (CSX-P), la cual podrá iniciar una vez culminada la implementación.
- El taller y/o curso propuesto deberá contar con una duración mínima de treinta (30) horas lectivas, académicas y/o pedagógicas las cuales podrán ser en la modalidad de sesiones de plataforma virtual síncronas.
- Todas las clases deberán poder grabarse para que los participantes puedan volver a reproducirlas desde su virtual classroom.
- Deberá contar con material descargable como diapositivas, manuales de laboratorio, papers, etc.
- Deberá contar con acceso al virtual classroom por tiempo limitado dentro de las fechas de inicio y finalización del curso.
- Se deberá incluir examen de certificación oficial para cualquiera de estas dos certificaciones Cybersecurity Certified Expert (CSCE) o CSX Cybersecurity Practitioner (CSX-P).
- Este taller y/o curso se llevará dentro de los sesenta (60) días calendarios de inicio de la operación del servicio, debiendo de emitir un acta de finalización del taller y/o curso, donde deberá de contar la firma de todos los participantes y del contratista.

SOBRE EL OPERADOR DEL SERVICIO IN-SITU

- Este servicio consiste en la provisión de Un (01) Operador de Servicio en las instalaciones de CORPAC (Av. Elmer Faucett Aeropuerto Internacional Jorge Chavez S/N Callao Perú - Zona sur, área de soporte técnico), el cual podrá desarrollar sus actividades de monitoreo, seguimiento y documentación de actividades del servicio de forma presencial.



- El contratista proporcionará Un (01) Operador de Servicio in situ los cuales cubrirán tres (03) días de la semana, siendo Lunes, Miércoles y Viernes de 8:30 am a 4:30 pm por el periodo de contrato de mil noventa y cinco (1095) días calendarios, a cargo de personal propio y especializado.
- El contratista asignará un recurso de coordinación y respuesta para los días y horas restantes, con la finalidad de cubrir 24 x 7 durante los 1095 días del contrato, el Operador de Servicio podrá brindar el servicio vía remota desde su base local o CyberSOC del fabricante.
- El contratista conforme asigna a su Operador de Servicio in situ en las instalaciones de CORPAC, será responsable por todos los gastos, seguros u otros ocasionados por el técnico residente. Asimismo, deberá contar con un equipo de cómputo propio y equipo móvil para brindar el servicio mencionado en este documento.

5.1.1.6 ATENCIÓN TÉCNICA Y NIVEL DE SERVICIO ESTABLECIDOS

- El servicio ofertado a través de una plataforma de CyberSOC con administración delegada deberá poder escalar un evento de interés a un incidente de forma automática y manual; los incidentes generarán una notificación por EMAIL y un ticket de mesa de ayuda o plataforma especializada cuando la integración esté habilitada.
- El servicio ofertado a través de una plataforma de CyberSOC administrada deberá poder escalar aún más un incidente, aislando el dispositivo y llamando al cliente. Cuando se detecta una ejecución potencialmente maliciosa en un dispositivo, el CyberSOC lo manejará como un incidente de Severidad 1 hasta que el contratista o personal asignado comunique lo contrario.
- Después de que el primer evento sospechoso/malicioso se convierta en un incidente, se deberán generar evidencia de que los analistas buscan otros eventos e incidentes inusuales y que lo corroboren. Bajo ningún criterio se recomienda archivar los eventos sin la evidencia técnica de un tratamiento de estos.
- Las aplicaciones integradas a la plataforma sirven como recopiladores de eventos; el CyberSOC deberá evaluar regularmente los eventos en las aplicaciones para buscar cualquier instancia que deba escalar a un incidente o crear una regla lógica para generar notificaciones automáticamente.
- Todo esto deberá estar configurado y evidenciado en la plataforma de gestión de servicios profesionales y gestión de incidentes para SOC.
- La plataforma deberá permitir configurar la zona horaria y personalizar horas críticas a fin de que el tiempo de detección, los patrones de telemetría y la zona horaria de la INSTITUCIÓN sean reconocidas por los analistas de CyberSOC Administrado y se puedan configurar acciones específicas. El CyberSOC Administrado deberá tener en cuenta la zona horaria del negocio y las ejecuciones fuera del horario laboral en el proceso de toma de decisiones.
- El CyberSOC iniciará una investigación en profundidad luego de cualquier incidente/evento de Severidad 1 para determinar si el historial de incidentes y los eventos en las aplicaciones presentan algún otro indicio de un entorno violado. Según lo que encuentre, el CyberSOC aislará los dispositivos si:
- El cliente no responde la llamada para confirmar que las acciones están autorizadas.
- El CyberSOC no puede determinar con 100 % de certeza que alguna etapa de un ataque no está en curso en función de los incidentes y eventos encontrados en el panel del cliente en ese momento.



NIVELES DE GRAVEDAD – EVENTOS / INCIDENTES				
SEVERIDAD	IMPACTO	DESCRIPCIÓN	RESPUESTA TÍPICA (DETECCIÓN/ NOTIFICACIÓN/ ACCIÓN)	SLA (ACUERDO DE NIVEL DE SERVICIO)
SEV1	CRÍTICA URGENTE	El sistema fue violado, ataque en curso.	2 min. / 5 min. / 10 min.	30 min.
SEV1	CRÍTICA	AV no pudo ponerse en cuarentena. Malicioso, sospechoso, ejecuciones o archivos inusuales. Entrada exitosa conexiones de direcciones IP de mala reputación o países monitoreados.	2 min. / 5 min. / 20 min.	45 min.
SEV2	IMPORTANT E	Actividad inusual, pero sin incumplimiento por parte de malintencionados se detectó una fiesta y ningún sistema los componentes estaban comprometidos.	2 min. / 10 min. / según sea necesario	No aplica
SEV3	MENOR	El sistema muestra intentos de inicio de sesión fallidos u otros eventos generados por la red del cliente sistemas o usuarios y no forman parte de una amenaza de ciberseguridad.	2 min. / 10 min. / según sea necesario	No aplica
SEV4	INFORMATI VA	No se observa ningún efecto malicioso en el sistema.	2 min. / según sea necesario / según sea necesario	No aplica



CONEXIONES DE RED TERRORISTA CIBERNÉTICA				
DETECTAR	ANALIZAR	REMEDIACIÓN / MITIGACIÓN		ACCIONES
CyberSOC	CyberSOC	CyberSOC	CyberSOC	CyberSOC
Conexión RDP sospechosa	Analizar detalles. Revisar la línea de tiempo. Identificar otros Eventos sospechosos.	Si se detecta un inicio de sesión exitoso, notifique al socio de TI. Si no está autorizado, aísle el dispositivo.	Si no está autorizado, cambie todos los usuarios, contraseñas con acceso al dispositivo. Ejecute un escaneo de antivirus completo. Investigar raíz causa. Aplicar políticas de acceso estrictas.	EMAIL/TICKET LLAMADA AISLAR
		Si se detecta fuerza bruta pero no inicio de sesión exitoso detectado, notificar Socio de TI.	Coloque RDP detrás de VPN. Actualizar sistema. Aplicar políticas de acceso estrictas.	EMAIL/TICKET
Conexión SQL sospechosa	Analizar detalles. Revisar la línea de tiempo. Identificar otros eventos sospechosos.	Si la conexión es exitosa, notifique al socio de TI. Si no está autorizado, aísle el dispositivo.	Si no está autorizado, cambie todos los usuarios contraseñas con acceso al dispositivo. Ejecute un escaneo antivirus completo. Aplicar estrictas políticas de acceso.	EMAIL/TICKET LLAMADA AISLAR
		Si la conexión está autorizada, notifique al socio de TI.	Ejecute un escaneo antivirus completo. aplicar estricto políticas de acceso.	EMAIL/TICKET LLAMADA
Conexiones entrantes sospechosas en 445 o 25 (SMB/SAMBA/Uso compartido de archivos de Windows) o 139 Servicio de sesión NetBIOS	Analizar detalles. Revisar la línea de tiempo. Identifica cualquier otro evento sospechoso.	Si la conexión es exitosa, notifique al socio de TI. Si no está autorizado, aísle el dispositivo.	Si no está autorizado, cambie todos los usuarios contraseñas con acceso al dispositivo. Ejecute un escaneo antivirus completo. Investigar la causa raíz de	EMAIL/TICKET LLAMADA AISLAR



			compromiso. Aplicar políticas de acceso estrictas.	
		Si la conexión está autorizada, notifique al socio de TI.	Si el Socio responde a nuestra llamada y confirma autorizado, o actual incidente o incidentes anteriores son resueltos antes de la convocatoria el CyberSOC no aislará el dispositivo.	EMAIL/TICKET LLAMADA

MONITOR DEL (XDR) ANTIVIRUS QUE SE INTEGRARÁ A LA PLATAFORMA DE CYBER SOC				
DETECTAR	ANALIZAR	REMEDIACIÓN / MITIGACIÓN		ACCIONES
CyberSOC	CyberSOC	CyberSOC	Cyber SOC	CyberSOC
SentinelOne Bitdefender Windows Defender Cylance Webroot Sophos Otros	Analizar detalles. Revisar la línea de tiempo. Identifique cualquier otro evento sospechoso.	Si se sabe que la amenaza es maliciosa y no se mitiga, aísle el dispositivo y notifique al socio de TI.	Se recomienda recuperar el sistema de una buena imagen anterior. Actualice las firmas y ejecute un análisis de antivirus completo del sistema.	EMAIL/TICKET LLAMADA AISLAR
		Si el hash se marca como malicioso y no se mitiga, notifique al socio de TI. Dependiendo de los detalles, aísle el dispositivo.	Si no está autorizado, se recomienda recuperar el sistema de una buena imagen anterior. Actualice las firmas y ejecute un análisis de antivirus completo del sistema.	EMAIL/TICKET LLAMADA AISLAR
		Si la amenaza se mitiga, notifique al socio de TI.	Revise la detección. Ejecute un escaneo AV completo del sistema. Identificar la fuente de la amenaza.	EMAIL/PSA
		Si la amenaza es una detección benigna o un falso positivo, notifique al socio de TI.	Suprimir si procede.	EMAIL/PSA



DETECCIÓN AVANZADA DE INFRACCIONES				
DETECTAR	ANALIZAR	REMEDIACIÓN / MITIGACIÓN		ACCIONES
CyberSOC	CyberSOC	CyberSOC	Cyber SOC	CyberSOC
Ejecución sospechosa de proxy binario firmado: a. Regsvr32.exe b. Mshta.exe c. Msiexec.exe d. Rundll32.exe	Analizar detalles. Revisar la línea de tiempo. Identifique cualquier otro evento sospechoso.	Si es malicioso, notifique al socio de TI. Aislar dispositivo.	Si no está autorizado, cambie las contraseñas de los usuarios con acceso al dispositivo. Investigue la causa raíz; dependiendo del resultado, reimagen.	EMAIL/TICKET LLAMADA AISLAR
		Si sospecha, notifique al socio de TI.	Si no está autorizado, cambie las contraseñas de los usuarios con acceso al dispositivo. Investigue la causa raíz; dependiendo del resultado, reimagen. Si está autorizado, resolver el incidente. Aplicar supresión de incidentes.	EMAIL/TICKET LLAMADA
Descarga sospechosa a través de PowerShell	Analizar detalles. Revisar la línea de tiempo. Identificar otros eventos o incidentes sospechosos.	Si es malicioso, notifique al socio de TI, aísle el dispositivo.	Si no está autorizado, cambie las contraseñas de los usuarios con acceso al dispositivo. Investigue la causa raíz; dependiendo del resultado, reimagen.	EMAIL/TICKET LLAMADA AISLAR
Cortafuegos de Windows desactivado	Analizar detalles. Revisar la línea de tiempo. Identificar otros eventos o incidentes sospechosos.	Si es malicioso, notifique al socio de TI, aísle el dispositivo.	Si no está autorizado, cambie las contraseñas de los usuarios con acceso al dispositivo. Investigue la causa raíz; dependiendo del resultado, reimagen.	EMAIL/TICKET LLAMADA AISLAR
Registro borrado e. PowerShell f. Windows g. Registro de eventos	Analizar detalles. Revisar la línea de tiempo. Identifique cualquier otro evento sospechoso.	Notifique al socio de TI. Aísle el dispositivo si hay otros IOC y el socio de TI no respondió la llamada.	Si no está autorizado, cambie las contraseñas de los usuarios con acceso al dispositivo. Investigue la causa raíz; dependiendo del resultado, reimagen.	EMAIL/TICKET LLAMADA
Creación de cuenta sospechosa	Analizar detalles. Revisar la línea de tiempo. Identifica cualquier otro	Notifique al socio de TI. Si no está autorizado/el socio no está disponible fuera del	Si no está autorizado, el dispositivo es comprometido; eliminar el nuevo cuenta(s), cambiar todos los usuarios	EMAIL/TICKET LLAMADA AISLAR



	eventos sospechosos.	horario de atención, aísle el dispositivo.	contraseñas con acceso al dispositivo. Ejecute un escaneo antivirus completo. Investigar raíz causa y dependiendo del resultado, puede que tenga que volver a crear la imagen.	
Manipulación de cuenta sospechosa	Analizar detalles. Revisar la línea de tiempo. Identificar otros eventos sospechosos.	Notifique al socio de TI. Si no está autorizado/el socio no está disponible, aísle el dispositivo.		EMAIL/TICKET LLAMADA AISLAR
Sistema de inhibición Recuperación h. vssadmin delete i. wmic delete j. wbadm delete k. bcdedit disable	Analizar imagen eliminar o deshabilitar Revisar la línea de tiempo. Analizar detalles. Identifica cualquier otro eventos sospechosos.	Llame al socio de TI. Si no está autorizado/el socio no accesible, aísle el dispositivo dependiendo de las horas de operación. Notifique al SOCIO DE TI si la ejecución es sospechosa.	Si no está autorizado, el dispositivo es comprometida. Ejecute un escaneo antivirus completo. Cambiar todas las contraseñas de usuario con acceso al dispositivo. Investigar raíz causa y dependiendo del resultado, puede que tenga que volver a crear la imagen. Si está autorizado, resuelva incidente. Aplicar supresión de incidentes.	EMAIL/TICKET LLAMADA AISLAR EMAIL/TICKET LLAMADA

DETECCIÓN IOC, HERRAMIENTAS SOSPECHOSAS Y SERVICIOS DE RED				
DETECTAR	ANALIZAR	REMEDIACIÓN / MITIGACIÓN		ACCIONES
CyberSOC	CyberSOC	CyberSOC	Cyber SOC	CyberSOC
Servicios de red sospechosos	Se detectó una red sospechosa.	Notifique al socio de TI.	Eliminar/desinstalar si no está autorizado. Ejecute un escaneo de antivirus completo en el sistema. Suprimir si procede.	EMAIL/TICKET
Herramientas sospechosas	Se detectó una herramienta sospechosa.	Notifique al socio de TI.	Eliminar/desinstalar si no está autorizado. Ejecute un escaneo antivirus completo en el sistema. Suprimir si procede.	EMAIL/TICKET



DETECCIÓN DE ARCHIVOS MALICIOSOS				
DETECTAR	ANALIZAR	REMEDIACIÓN / MITIGACIÓN		ACCIONES
CyberSOC	CyberSOC	CyberSOC	Cyber SOC	CyberSOC
Detección de archivos maliciosos/sospechosos	Analizar detalles. Revisar la línea de tiempo. Identificar cualquier otro evento sospechoso.	Si el archivo tiene una puntuación maliciosa alta o no se conoce (archivo no firmado, hash desconocido: vemos esto para una aplicación personalizada o malware de día 0) y el socio no responde la llamada para confirmar la autorización, aislar el dispositivo.	Eliminar/desinstalar si no está autorizado. Ejecute un escaneo antivirus completo en el sistema. Suprimir si procede.	EMAIL/TICKET LLAMADA AISLAR
		Si sospecha, notifique al socio de TI.	Si no está autorizado, elimine el archivo y ejecute un análisis antivirus completo. Si está autorizado, resuelva el incidente, suprima la notificación del incidente.	EMAIL/TICKET



ANALIZADOR DE INICIO DE SESIÓN DE OFFICE 365				
DETECTAR	ANALIZAR	REMEDIACIÓN / MITIGACIÓN		ACCIONES
CyberSOC	CyberSOC	CyberSOC	Cyber SOC	CyberSOC
Sospechoso inicio de sesión exitoso de O365 detectado	Analice los detalles (EMAIL/PSA y país). Revisar la línea de tiempo.	¿Inicio de sesión no autorizado? EMAIL/PSA Socio TI. Llame al evento por primera vez que se detecte.	Matar sesiones existentes. Habilite MFA para todos los usuarios en el arrendatario si no está activo. Agregue políticas de acceso condicional para bloquear por geolocalización.	EMAIL/TICKET LLAMADA
		¿Comportamiento esperado? Notifique al socio de TI.	Suprima la combinación EMAIL/PSA y país.	EMAIL/TICKET
Reglas de reenvío de correo electrónico/PSA sospechosas detectadas	Reglas de reenvío detectadas a EMAIL/PSA fuera del dominio corporativo.	Notifique al socio de TI.	Revisa la regla. Eliminar si no está autorizado. Suprimir si está autorizado.	EMAIL/TICKET
Detección de riesgos l. unlikelyTravel m. passwordSpray n. leakedCredentials o. impossibleTravel	Analizar detalles. Revisar la línea de tiempo.	Notifique al socio de TI.	Revise la alerta en Azure AD. Restablecer contraseña de usuario si no está autorizado. Suprimir si está autorizado.	EMAIL/TICKET

SERVICIOS 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 como plazo máximo en Lima Metropolitana					
Disponibilidad 24 x 7 x 365					
4 horas de atención como plazo máximo en provincia					
Registro de tickets de mesa de ayuda					
Tiempo máximo de registro del incidente, desde que son reportados		15 minutos			

5.2 ACTIVIDADES

El CONTRATISTA deberá ejecutar las siguientes actividades:

- Desarrollar el Plan de Trabajo del servicio.
- Implementar la plataforma de CyberSOC administrada en modalidad SaaS.
- Desplegar los agentes de monitoreo, detección y respuesta a incidentes, sobre el total de los nodos.
- Ejecutar de HACKING ÉTICO con remediación integral asistida de forma trimestral.
- Integrar las fuentes de datos (XDR, firewall, correo, switches, antivirus, etc.) a la plataforma CyberSOC.
- Ejecutar monitoreo 24x7 por parte del equipo de CyberSOC del fabricante.
- Ejecutar análisis de vulnerabilidades y reducción de superficie de ataque (externa e interna).
- Mantener y documentar la gestión de incidentes de seguridad con evidencia y trazabilidad.
- Ejecutar correlación de eventos con capacidades de SIEM-less y SOAR.
- Integrar capacidades de Cyber Threat Intelligence y monitoreo de dark web.
- Implementar sistema de clasificación, tratamiento y remediación de vulnerabilidades (basado en SSVC y CVSS).
- Brindar reportes mensuales y reportes bajo demanda (técnicos y ejecutivos).
- Implementar módulos de protección de fuga de información (IRM).
- Ejecutar plan de tratamiento conforme al marco NIST CSF e ISO 27001:2022.



5.3 PLAN DE TRABAJO

El CONTRATISTA deberá presentar al Área de Redes, Comunicaciones y Soporte Técnico el Plan de Trabajo correspondiente, en un plazo máximo de cinco (05) días calendario, contados a partir del día siguiente de la firma del contrato. La aprobación del Plan de Trabajo constituirá el inicio formal del proceso de implementación.

Como parte del Cronograma de trabajo, este deberá contener como mínimo las siguientes etapas:

- Elaboración del Plan de Trabajo.
- Implementación del Servicio.
- Operación del Servicio.
- Cierre del Servicio.

ETAPAS	MESES DE LAS ETAPAS											
	(5 días)	(1 mes)	Mes 01	Mes 02	Mes 03	Mes 04	Mes 05	Mes 06	Mes 34	Mes 35	Mes 36
Elaboración del Plan de Trabajo	Elaboración del Plan de Trabajo											
Implementación del Servicio		Implementación del Servicio										
Operación del Servicio			Operación del Servicio									
Cierre del Servicio												Cierre del Servicio

Nota: para efectos del presente, un mes equivale a 30 días calendario.

A continuación, se describe cada una de las etapas:

Etapas de Elaboración del Plan de Trabajo:

Consiste en definir cómo se ejecutará un proyecto, detallando actividades, plazos, responsables y recursos necesarios. Incluye la identificación de objetivos, el cronograma de actividades y los mecanismos de seguimiento. Esta etapa permite planificar de forma ordenada y estructurada el cumplimiento de los objetivos. También contempla la gestión de riesgos y la asignación eficiente de recursos. Es fundamental para garantizar el control y la coordinación del proyecto. Sirve como guía para todas las fases posteriores.

El plazo de esta etapa será de cinco (05) días calendarios contabilizados a partir del día siguiente de la firma del contrato.

Etapas de Implementación del Servicio:

El CONTRATISTA deberá realizar todas las implementaciones necesarias relativas a:

- Desplegar los agentes de monitoreo, detección y respuesta a incidentes, sobre los servidores seleccionados para este servicio:
- Asegurar la comunicación de estos con la plataforma administrada de CyberSOC.
- Descubrir y documentar el acceso privilegiado a estos recursos.
- Documentar el nivel de criticidad en función a la disponibilidad, integridad y privacidad de los activos.
- Desplegar los agentes de monitoreo, detección y respuesta a incidentes, sobre estaciones de trabajo con acceso privilegiado a recursos de misión crítica en la institución.
- Reconocer y clasificar los sistemas, aplicaciones y software; necesarios para la ejecución de los servicios.
- Proceder con la configuración de los sistemas a instalar del Contratista y la vinculación con el equipamiento y sistemas que se requieran.
- Proceder con las búsquedas de credenciales comprometidas sobre diversas fuentes incluyendo dark web, Telegram y otros.



- Proceder con la integración de fuentes y plataformas sobre el sistema de gestión integral SOAR o plataforma de CyberSOC administrada, a fin de procesar el correlacionamiento efectivo de antivirus, eventos de seguridad del sistema, firewall perimetral, directorio activo, inteligencia de amenazas sobre la dark web para detectar credenciales robadas e IPs de reputación peligrosa que interactúa con los servicios publicados de la institución. Se deben programar las tareas de reporte semanal y mensual de la plataforma de detección y respuesta a fin de evaluar estadísticamente el performance en el tiempo.
- Programar las actividades de reducción de superficie de ataque con objetivos de reducción del riesgo mensual.
- Establecer los canales de comunicación entre el Contratista y LA INSTITUCIÓN para la mesa de ayuda y registro de ocurrencias.

El plazo máximo para esta etapa es de treinta (30) días calendarios contabilizados a partir del día siguiente de suscrito la conformidad del Primer entregable que es el Plan de Trabajo.

El CONTRATISTA es responsable de la ejecución de esta etapa de Implementación del Servicio y debe presentar todo lo que corresponde de acuerdo con lo establecido en los TDRs. El esfuerzo de esta etapa no genera costos adicionales al servicio y debe ser asumido por el CONTRATISTA. Culminada esta etapa, se debe generar el Acta de inicio de la Etapa de Operación del Servicio.

Etapa de Operación del Servicio:

El Área de Redes, Comunicaciones y Soporte Técnico debe definir al equipo de trabajo responsable de mantener la operatividad del servicio documentando todos los incidentes y/o problemas sucedidos sobre el alcance del servicio a través de los canales establecidos en la etapa de implementación del servicio. El CONTRATISTA está en la obligación de comunicar el registro de tickets en un plazo máximo de 15 minutos de reportada la incidencia. La mesa de ayuda debe estar operativa 24x7x365 para el registro de ocurrencias

Esta etapa de operación inicia luego de concluida la etapa de implementación y consiste en la parte de ejecución del servicio de monitoreo y alerta de seguridad cybersoc.

Esta etapa tiene una duración de mil noventa y cinco (1095) días calendario. Se inicia luego de culminar la etapa de implementación y al día siguiente de suscribir el Acta de inicio de la Etapa de Operación del Servicio.

La operación debe tener ciclos de 30 días calendario. Al final de cada ciclo se debe presentar reporte de cada una de las actividades del servicio de monitoreo y alerta de seguridad cybersoc.

COBERTURA DEL SERVICIO

- Monitoreo efectivo de agentes de comunicación de la plataforma de detección y respuesta
- Monitoreo efectivo de agentes de comunicación de la plataforma de prevención y reducción de superficie de ataque.
- Monitoreo y correlación efectiva de fuentes antivirus, EDR y eventos del sistema.

MONITOREO AVANZADO

- Tratamiento y correlación de eventos recopilados por semana.
- Configuración de listas blancas, listas negras.
- Análisis de eventos de seguridad que generen incidentes y/o alertas.
- Gestión de tickets sobre plataforma de gestión de incidentes.

INTELIGENCIA DE AMENAZAS, THREAT HUNTING Y HACKING ÉTICO

- Identificación, registro y acción sobre conexiones con redes ciberterroristas.



- Reporte de riesgos, amenazas y credenciales comprometidas (Correo, sistemas y plataformas) en la dark web.
- Activos expuestos a riesgo cibernético través de vulnerabilidades, configuraciones débiles y anomalías.
- Actividad de hacking ético caja negra y caja gris sobre activos específicos expuestos y ejercicios de pentesting.
- Actividades de reducción de superficie de ataque interna y externa.

MEJORA CONTINUA

- Evaluación de cumplimiento
- Definición de objetivos
- Asesoría de cumplimiento y maduración de niveles.
- Concientización de ciberseguridad a través de boletines informativos publicados en la corporación semanalmente.

Debe contener un apartado, de ser el caso, de los hechos resaltantes que han sucedido en dicho ciclo.

Además, debe tener el reporte de todas las actividades conforme los niveles de servicio establecidos (SLA) descritos.

El CONTRATISTA debe proveer un sistema de atención de mesa de ayuda, registrando todos los incidentes. LA INSTITUCIÓN debe reportar todos los incidentes o problemas sucedidos sobre el alcance del servicio a través de los canales establecidos en la etapa de implementación del servicio. El CONTRATISTA está en la obligación de comunicar el registro de tickets en un plazo máximo de 15 minutos de reportada la incidencia. La mesa de ayuda debe estar operativa 24x7x365 para el registro de ocurrencias.

Etapas de Cierre del Servicio:

Periodo de tiempo en el cual el CONTRATISTA ejecutará las actividades necesarias para el traslado o migración de los recursos contemplados en el presente servicio. Esta fase se ejecutará dentro de la Etapa de Operación del Servicio, teniendo una duración de sesenta días (60) calendarios como máximo.

- Las etapas deben incluir la siguiente información como mínimo:
- Nombre de la etapa
- Nombre de la actividad
- Plazos para cada actividad
- Duración de la actividad
- Fecha de inicio de la actividad
- Fecha de fin de la actividad
- Responsables de la actividad

Para cada una de las etapas del servicio el CONTRATISTA debe identificar los riesgos que afecten cada una de sus etapas. El Plan de trabajo debe contener las etapas de implementación, operación y cierre del servicio.

5.4 SEGUROS

El Operador de Servicio que estará in situ en las instalaciones de CORPAC, deberá contar con un seguro de vida o riesgos, asumido por el contratista, por un plazo de 1095 días calendarios. Esta se presentará a la suscripción del contrato, tales como el seguro de accidentes personales, seguro complementario de trabajo de riesgo, entre otros.



5.5 LUGAR Y PLAZO DE PRESTACIÓN DEL SERVICIO

5.6.1 Lugar

La ejecución del servicio se realizará en la sede central de CORPAC S.A ubicada en la Av. Elmer Faucett N° 3400 Aeropuerto Internacional Jorge Chavez Zona Sur. (Edificio Ex OACI)

5.6.2 Plazo

A continuación, se detallan los plazos correspondientes a cada etapa del servicio:

Plazo para el plan de trabajo

El plazo máximo para esta etapa es de cinco (5) días calendarios, contabilizados a partir del día siguiente de la firma del contrato

Plazo de Implementación del Servicio:

El plazo máximo para esta etapa es de treinta (30) días calendarios contabilizados a partir del día siguiente de suscrito la conformidad del Primer entregable que es el Plan de Trabajo.

Plazo de Operación del Servicio:

El plazo para la ejecución del servicio en su etapa operativa es de mil noventa y cinco (1095) días calendario, contabilizados a partir del día siguiente de la suscripción del Acta de inicio de la Etapa de Operación del Servicio, una vez culminada satisfactoriamente la etapa de implementación.

Dentro de ese plazo, también se realizará:

- Servicio integral para la mejora de la seguridad de la información y ciberseguridad según la NIST CSF 2.0 o NIST IR 8376.
- Dentro de los 30 días calendarios posteriores de la implementación del CyberSOC se presentará el primer informe de cumplimiento.
- Servicio de operación análisis de ciberseguridad IN-SITU
Dentro de los 10 días calendarios, posteriores de la implementación del CyberSOC iniciaría formalmente el analista responsable en los horarios establecidos por la vigencia del contrato.
- Ejercicios de HACKING ÉTICO con remediación integral asistida de forma trimestral a través de la plataforma de gestión colaborativa segura.
 1. Dentro de los 30 días calendarios posteriores de la implementación del CyberSOC se presentaría formalmente el primer ejercicio de hacking ético con remediación asistida.
 2. El ejercicio deberá ejecutarse tres (03) veces al año, y deberá mantener activo detalles de los ejercicios y remediaciones en una plataforma de gestión colaborativa segura durante la vigencia del contrato.

C) Plazo de Cierre del Servicio:

El plazo para la etapa de cierre tendrá una duración de sesenta días (60) calendarios como máximo, dentro de la Etapa de Operación del Servicio.



5.6.2.1 Entregables del Servicio

Los entregables deberán ser presentados por medio digital en formato PDF, en Mesa de Partes Virtual de CORPAC, dirigido a la Gerencia de Tecnología de la Información y Comunicaciones y Área de Redes, Comunicaciones y Soporte Técnico; dentro de los siguientes plazos:

ENTREGABLE N°	PRODUCTO	PLAZO DE ENTREGA
PRIMERO	Plan de trabajo	Máximo a los 05 días calendario, contabilizados a partir del día siguiente de suscrito el contrato.
SEGUNDO	Informe de Implementación del Servicio	Máximo a los 30 días calendario, el mismo que inicia desde el día siguiente de suscrito la conformidad del primer entregable que es el Plan de Trabajo.
TERCERO	Informes de Operación del Servicio	<p>Cada 30 días calendario, el mismo que inicia luego de culminar la etapa de implementación y al día siguiente de suscribir el Acta de inicio de la Etapa de Operación del Servicio. Este reporte será periódico cada 30 días, por los 1095 días que dure la etapa de operación del servicio.</p> <ul style="list-style-type: none"> - Informe de servicio integral para la mejora de la seguridad de la información y ciberseguridad según la ISO 27001:2022. - Detalle de incidencias y actividades realizadas como consecuencia del servicio de operación del analista de ciberseguridad IN-SITU. - Informes de resultados de los ejercicios de HACKING ÉTICO con remediación integral asistida de forma trimestral. - Informes de los hechos significativos señalados en el numeral 5.3 Plan de Trabajo – Etapa de Operación del Servicio.
CUARTO	Cierre del Servicio	La etapa de cierre tendrá una duración de 60 días calendarios como máximo. Incluye la entrega de un informe final con resultados, estadísticas e incidentes gestionados. Finalmente, se firma un acta de conformidad que valida el cumplimiento del servicio.

El informe de todos productos y entregables deberá ser remitida vía correo electrónico y/o publicado en link de acceso en nube para descarga, debidamente organizados e identificados, una vez hayan sido presentado por mesa de partes virtual. Debe Adjuntarse con:

- Los archivos en formatos originales (MS Word, MS Excel, MS Project, MS Visio, etc.)
- La versión final de los productos, en formato PDF con firma digital de los responsables del equipo técnico del contratista.



6 RECURSOS A SER PROVISTOS POR EL CONTRATISTA

6.1 Equipamiento

A. Equipamiento estratégico

Como parte del servicio del Cybersoc, el CONTRATISTA deberá implementar en la etapa de implementación dentro de los 30 días calendarios, posteriores a la conformidad del Plan de Trabajo, considera la provisión, instalación y puesta en operación un sistema de Video Wall de propiedad del contratista, el cual se integrará a la red corporativa; para la visualización de la operación del servicio (con todos los componentes de seguridad implementados) por parte del personal de la Gerencia de Tecnologías de la Información y comunicaciones. El sistema de video wall será implementado en la Sala GTIC Ex OACI, donde se encontrará el operador del servicio in situ. El sistema de Video Wall debe contar con su software para visualización en los monitores, el cual debe estar integrado en la red para visualizar los sistemas del Cybersoc.

Características Mínimas

Se requiere 1 sistema de Video Wall, debe contar con al menos 04 pantallas, con sus respectivos rack y controlador de video, se instalarán en la sala destinada a la operación del servicio en edificio Ex OACI para la monitorización de los servicios del Cybersoc implementado:

Pantallas características:

- 4 und - Tamaño de pantalla 46", Tecnología LED
- Resolución mínima del Panel 1920 x 1080 (16: 9) Full HD
- Brillo de pantalla 500 cd/m2
- Relación de contraste 3500:1
- Ángulo de visión (horizontal/vertical) 178°/178°
- Orientación Paisaje/Retrato
- Tiempo de respuesta (8ms G-a-G).
- Fuente de alimentación AC 100 - 240 V ~ (+/- 10%), 50/60 Hz
- Módulo de hardware especial Wi-Fi Embedded.

Características Controlador de video:

- soportar mínimo 04 pantallas, debe ser administrable vía web, Resolución 800 x 480, 2048 x 1080 (1080p) de tipo Pared de TV independiente
- Hardware apropiado de última generación para un de rendimiento optimizado.
- Debe contar con Puerto Ethernet para su conexión a la red corporativa.
- Debe operar con Navegadores Internet Explore, Mozilla, Chrome actualizados publicados en el mercado.
- Debe contar con Sistema operativo Embebido.
- De incluir todas sus licencias.

El equipamiento estratégico será de propiedad del contratista y operará por la duración del servicio 1095 días y al final del servicio será retirado de la corporación por el mismo contratista.

B. OTRO EQUIPAMIENTO

No corresponde

6.2 Infraestructura estratégica (De corresponder)

No corresponde



6.3 Personal (De corresponder)

A. Personal clave

Para la prestación del servicio con la disponibilidad requerida de 24x7x365 se considerará el siguiente personal clave:

Nº	PERSONAL CLAVE	ROL/FUNCION	FORMACION ACADEMICA	EXPERIENCIA	CAPACITACIÓN Y/O CERTIFICACIÓN
01	UN (01) LIDER DEL PROYECTO Y RESPONSABLE DE LA AUDITORIA Y CUMPLIMIENTO DE LA NORMA ISO27001:2022 – EXTERNO	<ul style="list-style-type: none"> Responsable de asegurar el cumplimiento con base en las buenas prácticas de los objetivos planteados para el proyecto. Encargado de elaborar la planificación del proyecto. Encargado de la elaboración y presentación de toda la documentación y entregables del proyecto Interlocutor responsable para todas las coordinaciones y comunicaciones del proyecto con los involucrados. Liderará por parte del CONTRATISTA el servicio que se está ofertando. 	Titulado Universitario Colegiado en Computación e Informática y/o Sistemas y/o Electrónica y/o Redes y Comunicaciones y/o Telecomunicaciones.	<ul style="list-style-type: none"> Debe contar con más de cuatro (04) años de experiencia relacionada a Servicios de ciberseguridad y/o seguridad de la información. Debe presentar evidencia de por lo menos quince (15) auditorías realizadas a diferentes empresas. 	<ul style="list-style-type: none"> Certificado "Information Security Foundation based on ISO/IEC 27002" Certificado y/o Taller y/o Diploma y/o Curso de formación con una cantidad de 18 horas lectivas, académicas y/o pedagogías en Gestión de la Ciberseguridad desde un enfoque corporativo, bajo los lineamientos de la ISO 27032. Certificado y/o Taller y/o Diploma y/o Curso de formación con una cantidad de 18 horas lectivas, académicas y/o pedagogías en Gestión y Administración de la seguridad de la información, bajo el enfoque de la norma ISO 27001. Debe presentar certificación oficial del fabricante o distribuidor local autorizado de todas las



					plataformas ofertadas.
02	UN (01) GESTOR DEL SERVICIO – EXTERNO	<ul style="list-style-type: none"> • Consolidar y presentar los resultados obtenidos de la plataforma y/o tecnología utilizada para brindar capacidades de predictibilidad de un ataque cibernético. • Consolidar y presentar los resultados obtenidos de la plataforma y/o tecnología utilizada para el pentesting y reducción de superficie de ataque externa. • Consolidar y presentar los resultados obtenidos de la plataforma y/o tecnología utilizada para el reconocimiento y gestión de riesgo basado en vulnerabilidades, configuraciones débiles y anomalías. • Consolidar y presentar los resultados obtenidos de la plataforma y/o tecnología utilizada para brindar capacidades de detección y respuesta ante ataques cibernéticos, mostrando evidencia del correlacionamiento de eventos de múltiples fuentes 	Titulado Universitario Colegiado en Computación e Informática y/o Sistemas y/o Electrónica y/o Redes y Comunicaciones y/o Telecomunicaciones.	<ul style="list-style-type: none"> • Debe contar con más de tres (03) años de experiencia relacionada a Servicios de ciberseguridad y/o seguridad de la información. 	<ul style="list-style-type: none"> • Certificado PMP o "Scrum Master Certified" VIGENTE • Certificado "Certified Cyber Security Management Professional ISO 27032" • Certificado "ITIL Foundation Certificate in IT Service Management" • Certificado de "Taller de Gestión de CIBERCRISIS", con una duración de 08 horas lectivas, académicas y/o pedagogías. • Debe presentar certificación oficial del fabricante o distribuidor local autorizado de todas las plataformas ofertadas.



		y alertas sobre servicios o aplicaciones sospechosas.			
03	UN (01) ESPECIALISTA EN CIBERSEGURIDAD Y HACKING ÉTICO – EXTERNO	<ul style="list-style-type: none"> • Ejecutar ejercicios de hacking ético en modalidad de caja negra y caja gris sobre la red de CORPAC S.A. • Organizar y presentar los resultados obtenidos, mediante un informe. • Liderar actividades de remediación y/o mitigación de incidentes cibernéticos. • Absolver consultas técnicas y dar soporte a incidentes reportados en CORPAC S.A. • Elaborar directivas y concientización de la ciberseguridad a través de informativos para los usuarios de CORPAC S.A. 	Técnico Titulado y/o bachiller y/o titulado en; Computación e Informática y/o Sistemas y/o Electrónica y/o Redes y Comunicaciones y/o Telecomunicaciones.	Debe contar con más de tres (03) años de experiencia relacionada a Servicios de ciberseguridad y/o seguridad de la información.	<ul style="list-style-type: none"> • Certificado Oficial "Certified Ethical Hacker (CHE)" VIGENTE. • Certificado realizado por una institución de formación especializada de Taller y/o Curso y/o Programa de Especialización en CIBERSEGURIDAD DEFENSIVA con una duración mínima de ciento veinte (120) horas lectivas, académicas y/o pedagogías. • Certificado de "Taller de Gestión de CIBERCRISIS", con una duración de 08 horas lectivas, académicas y/o pedagogías. • Debe presentar certificación oficial del fabricante o distribuidor local autorizado de todas las plataformas ofertadas.
04	UN (1) OPERADOR DEL SERVICIO IN-SITU	<ul style="list-style-type: none"> • Responsable de liderar la operación del servicio que se debe brindar • Responsable de asegurar el cumplimiento de todos los niveles de servicio requeridos. 	Bachiller y/o Titulado Universitario en Sistemas Electrónica, Informática y/o Redes y Comunicaciones y/o similares.	Deberá contar con una experiencia profesional mínima de dos (02) años en implementaciones de ciberseguridad (Análisis de vulnerabilidad y/o Pentesting	<ul style="list-style-type: none"> • Debe presentar certificación oficial del fabricante o distribuidor local autorizado de todas las plataformas ofertadas.



		<ul style="list-style-type: none"> • Es el interlocutor de todas las operaciones técnicas del servicio y que coordinará con CORPAC todas las actividades del Servicio. • Informar las posibles amenazas críticas a la red de datos de CORPAC con respecto a la descripción del alcance del servicio • Dirigirá al equipo NOC en las medidas de operación y mitigación propias del servicio 		y/o Ethical Hacking y/o monitoreo SOC - Security Operación Center, Prevención de pérdida de datos, entre otros)	
--	--	---	--	---	--

NOTA:

- El documento de auditoria deberá ser presentado en la etapa de perfeccionamiento de contrato.
- Las certificaciones serán presentadas en la etapa de perfeccionamiento de contrato.
- La colegiatura y la habilitación profesional será presentada para el inicio del servicio.

B. Otro personal

No corresponde

C. PROCEDIMIENTO PARA CAMBIO DE PERSONAL CLAVE

Para la prestación de la contratación correspondiente, el CONTRATISTA utilizará el personal calificado especificado en su oferta, no estando permitido cambios, salvo por razones de caso fortuito o fuerza mayor debidamente comprobadas, sustentando los motivos mediante un informe que refrende dicho cambio. En estos casos, el Contratista deberá proponer a la Entidad, por escrito, a través de mesa de partes virtual (**Enlace mesa de partes virtual:** <https://extranet.corpac.gob.pe/mesa-partesvirtual/Account/Login?ReturnUrl=%2Fmesa-partes-virtual%2F>) para su aprobación por parte de la Gerencia de Tecnologías de la Información y Comunicaciones, el que deberá reunir y acreditar calificaciones profesionales iguales o superiores al personal requerido.

7 OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

7.2 Otras obligaciones

7.2.1 Otras obligaciones del contratista

Como parte del servicio del Cybersoc, el contratista deberá implementar en la etapa de implementación dentro de los 30 días calendarios, posteriores a la conformidad del Plan de Trabajo (considera la provisión, instalación y puesta en operación) un sistema de Video Wall de propiedad del contratista, el cual se integrará a la red corporativa; para la visualización de la operación del servicio (con todos los componentes de seguridad implementados) por parte del personal de la Gerencia de Tecnologías de la Información. Será implementado en la Sala



Ex OACI, donde se encontrará el operador del servicio in situ. El sistema de Video Wall debe contar con su software para visualización en los monitores, el cual debe estar integrado en la red para visualizar los sistemas del Cybersoc.

7.2.2 OTRAS OBLIGACIONES DE LA ENTIDAD

La entidad (por medio del área usuaria) deberá de brindar todas las facilidades al contratista para la ejecución del servicio.

7.3 ADELANTOS (De corresponder)

No corresponde

7.4 SUBCONTRATACIÓN (De corresponder)

No corresponde

7.5 CONFIDENCIALIDAD

El Contratista deberá de brindar la reserva absoluta en el manejo de la información y documentación a la que tenga acceso y que se encuentre relacionada con la prestación, quedando prohibido revelar dicha información a terceros.

El Contratista del servicio se compromete a no divulgar ni transferir a terceros la información que CORPAC S.A. le brinde para la ejecución de la prestación a su cargo, sin la autorización previa y por escrito de la CORPAC. Caso contrario, el CONTRATISTA del servicio responderá por los daños y perjuicios causados.

Toda información a que tenga acceso el contratista, así como su personal, es estrictamente confidencial, el contratista y su personal deberá mantener las reservas del caso y no transmitirla a ninguna persona (natural o jurídica) sin la autorización expresa y por escrito de la entidad. Caso contrario, el contratista del servicio responderá por los daños y perjuicios causados. El tiempo de confidencialidad es indefinido.

7.6 PROPIEDAD INTELECTUAL

El CONTRATISTA no tendrá ningún título, patente u otros derechos de propiedad en ninguno de los documentos preparados, tales derechos pasaran a ser propiedad de CORPAC.

7.7 MEDIDAS DE CONTROL DURANTE LA EJECUCIÓN CONTRACTUAL

No corresponde

7.8 CONFORMIDAD DE LA PRESTACIÓN

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025. La conformidad será otorgada por el Área de Redes, Comunicaciones y Soporte Técnico y la Gerencia de Tecnología de la Información y comunicaciones de CORPAC, en un plazo máximo de siete (7) días calendarios, computados desde el día siguiente de recibido el entregable.

La conformidad del servicio será otorgada cada 30 días calendarios, previo informe del CONTRATISTA, durante el tiempo de la etapa de operación del servicio por mil noventa y cinco (1095) días calendarios, misma que será emitida por el Área de Redes, Comunicaciones y Soporte Técnico y la Gerencia de Tecnología de la Información y comunicaciones de CORPAC.



Cumplido los mil noventa y cinco (1095) días calendario correspondientes a la etapa de operación del servicio, por el Área de Redes, Comunicaciones y Soporte Técnico y la Gerencia de Tecnología de la Información y comunicaciones de CORPAC, emitirá la conformidad final.

De existir observaciones, la entidad contratante comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar de 8 días calendarios, contabilizados desde el día siguiente de la notificación de las observaciones. Subsanadas las observaciones dentro del plazo otorgado, no corresponde la aplicación de penalidades.

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 sin considerar los días en los que pudiera incurrir la Entidad para efectuar las revisiones y notificar las observaciones correspondientes.

Este procedimiento no resulta aplicable cuando los bienes, servicios y/o consultorías manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso la entidad contratante no efectúa la recepción o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

La recepción conforme de la entidad contratante no obsta su derecho a reclamar posteriormente por defectos o vicios ocultos, de acuerdo con lo dispuesto en el literal c) del numeral 69.2 del artículo 69 de la Ley de Contrataciones del Estado.

ENTREGABLE N°	PRODUCTO	CONFORMIDAD
PRIMERO	Plan de trabajo	Máximo a los 03 días calendario, contabilizados a partir de recibido el Plan de Trabajo, conformidad emitida por el Área de Redes, Comunicaciones y Soporte Técnico y la Gerencia de Tecnología de la Información y comunicaciones de CORPAC
SEGUNDO	Informe de Implementación del Servicio	Máximo a los 03 días calendario, contabilizados a partir de recibido el Informe de Implementación, conformidad emitida por el Área de Redes, Comunicaciones y Soporte Técnico y la Gerencia de Tecnología de la Información y comunicaciones de CORPAC.
TERCERO	Informes de Operación del Servicio	Máximo a los 07 días calendario, cada 30 días calendarios, previo informe del CONTRATISTA, conformidad emitida por el Área de Redes, Comunicaciones y Soporte Técnico y la Gerencia de Tecnología de la Información y comunicaciones de CORPAC.
CUARTO	Cierre del Servicio	Máximo a los 03 días calendario, previo informe final de resultados CONTRATISTA y Acta de Cierre del Servicio, conformidad emitida por el Área de Redes, Comunicaciones y Soporte Técnico y la Gerencia de



		Tecnología de la Información y comunicaciones de CORPAC.
--	--	--

7.9 MODALIDAD DE PAGO

La presente contratación se rige por la modalidad de suma alzada, de conformidad con el artículo 130 del Reglamento.

7.10 FORMA DE PAGO

La entidad contratante paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días hábiles siguientes de otorgada la conformidad por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles.

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

La Entidad contratante realizará el pago de la contraprestación pactada a favor del contratista en, PAGOS MENSUALES, **se realizará cada 30 días por los 1095 días calendarios**, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

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

- Documento en el que conste la conformidad de la prestación efectuada suscrita por el servidor responsable por el Área de Redes, Comunicaciones y Soporte Técnico y la Gerencia de Tecnología de la Información y comunicaciones de CORPAC.
- Comprobante de pago.
- Informe del CONTRATISTA del mes correspondiente.

Se precisa que la documentación debe ser presentada por el contratista es conforme lo siguiente:

Para el primer pago la Entidad deberá de contar con:

- Comprobante de pago
- Informe del contratista del entregable correspondiente
- Acta de conformidad por parte de la entidad
- Presentación del plan de trabajo
- Informe de implementación.

Para el segundo pago, la entidad deberá de contar con:

- Comprobante de pago
- Informe del contratista del entregable correspondiente
- Acta de conformidad por parte de la entidad
- Acta de finalización del taller y/o curso.



Para el tercer y hasta el último pago la Entidad deberá de contar con:

- Comprobante de pago
- Informe del contratista del mes correspondiente
- Acta de conformidad por parte de la entidad del mes correspondiente
- informe final de resultados, estadísticas e incidentes gestionados (ultimo pago).

En caso de retraso en el pago por parte de la Entidad, salvo que se deba acaso fortuito o fuerza mayor, EL CONTRATISTA tiene derecho al pago de intereses legales conforme a lo establecido en el artículo 67 de la Ley N° 32069, Ley General de Contrataciones Públicas.

Salvo los documentos que emite la entidad contratante, es decir, de recepción y verificación, así como de conformidad, el contratista debe presentar la documentación restante a través de la Mesa de Partes Virtual de CORPAC S.A., dentro de los horarios de trabajo establecidos 8:30 a 16:30 horas. Pasado dicho horario, los usuarios pueden presentar documentación, pero se dará por recibida a partir del día hábil siguiente.

Enlace mesa de partes virtual: <https://extranet.corpac.gob.pe/mesa-partesvirtual/Account/Login?ReturnUrl=%2Fmesa-partes-virtual%2F>

7.11 FÓRMULA DE REAJUSTE (DE CORRESPONDER)

No corresponde.

7.12 PENALIDAD DE MORA

Conforme al artículo 120 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

7.13 OTRAS PENALIDADES APLICABLES

Adicionalmente a la penalidad por mora, se aplicarán las siguientes penalidades:

Otras Penalidades			
N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
1	Realizar cambios de personal asignado al servicio, sin contar con la aprobación de la Gerencia de Tecnología de la Información y Comunicaciones	10% de la UIT. Se aplicará la penalidad por cada ocurrencia	Mediante informe de la Gerencia de Tecnología de la Información y Comunicaciones, la cual supervisará el servicio.



Por incumplimientos de Niveles de Servicio (SLA)

Penalidades en SERVICIOS DE CYBERSOC					
Servicio		SLA		Penalidad	
Monitoreo de salud de la plataforma		Disponibilidad diaria 24x7x365		Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.	
Monitoreo avanzado tiempo real y correlación de eventos de seguridad		Disponibilidad diaria 24x7x365		Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.	
Cyber Threat Intelligence (Inteligencia de Ciberseguridad)		Disponibilidad diaria 24x7x365		Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.	
Threat Hunting		Disponibilidad diaria 24x7x365		Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.	
Alerta Temprana		Disponibilidad diaria 24x7x365		Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.	
Portal de Supervisión		Disponibilidad diaria 24x7x365		Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.	
Penalidades en Advanced Security Incident Response (Respuesta Avanzada a Incidentes)					
Registro de incidente: Ticket generado por	Tiempo promedio de detección e inicio del análisis	Tiempo promedio de contención	Tiempo promedio de reparación	Tiempo promedio de resolución	Análisis de repercusiones



CONTRATISTA					
<= 15 minutos de reportado el incidente	< 30 minutos	< 45 minutos	< 3 horas	< 6 horas	Dentro de las 48 horas de resuelto el incidente.
Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	Penalidad: 3% de UIT por cada ocurrencia de incumplimiento
Penalizaciones por Tiempos de Atención Off-Site					
Disponibilidad 24 x 7 x 365			Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.		
2 horas de atención como plazo máximo en Lima Metropolitana			Penalidad: 3% de UIT por cada ocurrencia de incumplimiento		
4 horas de atención como plazo máximo en provincias			Penalidad: 3% de UIT por cada ocurrencia de incumplimiento		
Penalizaciones por Registro de tickets de mesa de ayuda					
Tiempo máximo de registro del incidente, desde que son reportados		15 minutos		Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	

La suma de la aplicación de las penalidades por mora y otras penalidades no debe exceder el 10% del monto vigente del contrato, de ser el caso, del ítem correspondiente.

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

7.14 RESPONSABILIDAD POR VICIOS OCULTOS

En los contratos de bienes y servicios, el contratista es responsable por la calidad ofrecida y por los vicios ocultos del servicio por mil noventa y cinco (1095) días calendario, contados a partir de la conformidad otorgada por la entidad contratante, de acuerdo con el Artículo 69° de la Ley General de Contrataciones Públicas – N.º 32069. La recepción conforme de la entidad contratante no obsta su derecho a reclamar posteriormente por defectos o vicios ocultos, de acuerdo con lo dispuesto en el literal c) del numeral 69.2 del artículo 69 de la Ley.

7.15 SISTEMA DE ENTREGA (DE CORRESPONDER)

No Aplica.



7.16 HOMOLOGACIÓN DEL REQUERIMIENTO

El presente requerimiento no está definido en una ficha de homologación del listado de requerimientos homologados implementado por PERU COMPRAS, así mismo el requerimiento no se encuentra en una ficha técnica del Lista de Bienes y Servicios Comunes, o en el Catálogo Electrónico de Acuerdos Marco.

7.17 RESOLUCIÓN DE CONTRATO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas.

De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES procederán de acuerdo con lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF

7.18 CLÁUSULA GESTIÓN DE RIESGOS (De corresponder en caso el requerimiento se encuentre segmentado como Estratégico y según lo establecido en el artículo 128 del Reglamento de Contratación Pública)

No corresponde.

7.19 SOLUCIÓN DE CONTROVERSIAS CONTRACTUALES:

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante arbitraje.

Para dicho efecto, el postor ganador de la buena pro selecciona a uno de las siguientes Instituciones Arbitrales para administrar el arbitraje:

- Centro de Arbitraje del OSCE – Organismo Supervisor de las Contrataciones del Estado
- Centro de Análisis y Resolución de Conflictos -PUCP.
- Centro de Arbitraje de la cámara de Comercio de Lima.

3.5. REQUISITOS DE CALIFICACIÓN

2.5.1. REQUISITOS DE CALIFICACIÓN OBLIGATORIOS

B. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a S/ 5,600,000.00 (cinco millones seiscientos mil), por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los quince (15) años anteriores a la fecha de la presentación de ofertas que se computa desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes:

- Servicio o suscripción de plataformas de Seguridad informática o SOC.
- Servicio de suscripción para una plataforma de correlacionador de eventos (SIEM) y SOC delegada tipo SOAR para el monitoreo, prevención, detección, y respuesta ante incidentes cibernéticos con seguridad gestionada.
- Servicio o suscripción de plataformas de Ciberseguridad o gestión de riesgo cibernético.
- Licencias antivirus y/o antispam y/o EDR y/o XDR.
- Soluciones de gestión de riesgo cibernético.
- Suscripción de plataformas de continuidad de negocio y/o respaldo con doble capa
- Servicios de hacking ético.
- Servicios o suscripción de SOC Administrado o Managed SOC.

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con constancia 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 pago⁷, correspondientes a un máximo de veinte contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados⁸, para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.

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° 11** 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 quince (15) 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.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de 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° 14**.

Las personas jurídicas resultantes de un proceso de reorganización societaria no pueden acreditar como experiencia del postor en la especialidad aquella que le hubieran transmitido como parte de dicha reorganización las personas jurídicas sancionadas con inhabilitación vigente o definitiva.

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

⁷ 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. Es válido el sello colocado por el cliente del postor (sea utilizando el término “cancelado” o “pagado”).

⁸ Se entiende “privados” como aquellos que no son entidades contratantes.

de suscripción del contrato, de emisión de la orden de servicio o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo N° 11** referido a la Experiencia del Postor en la Especialidad.

Advertencia

En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que ejecutan conjuntamente el objeto del contrato.

2.5.2. REQUISITOS DE CALIFICACIÓN FACULTATIVOS

C. CAPACIDAD TÉCNICA Y PROFESIONAL

C.1. EXPERIENCIA DEL PERSONAL CLAVE

Requisitos:

- El **LIDER DEL PROYECTO Y RESPONSABLE DE LA AUDITORÍA Y CUMPLIMIENTO DE LA NORMA ISO 27001:2022 – EXTERNO** debe acreditar cuatro (04) años de experiencia relacionada a Servicios de ciberseguridad y/o seguridad de la información.
- El **GESTOR DEL SERVICIO – EXTERNO** debe acreditar más de tres (03) años de experiencia relacionada a Servicios de ciberseguridad y/o seguridad de la información.
- El **ESPECIALISTA EN CIBERSEGURIDAD Y HACKING ÉTICO – EXTERNO** debe acreditar más de tres (03) años de experiencia relacionada a Servicios de ciberseguridad y/o seguridad de la información.
- El **OPERADOR DE SERVICIO IN-SITU** debe acreditar mínimo dos (02) años de experiencia en implementaciones de ciberseguridad (Análisis de vulnerabilidad y/o Pentesting y/o Ethical Hacking y/o monitoreo CyberSOC – Security Operación Center, Prevención de pérdida de datos, entre otros).

Acreditación:

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

Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.

En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.

Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco años anteriores a la fecha de la presentación de ofertas.

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

C.2. CALIFICACIONES DEL PERSONAL CLAVE

C.2.1 Formación académica

Requisitos:

- Titulado Universitario Colegiado en Computación e Informática y/o Sistemas y/o Electrónica y/o Redes y Comunicaciones y/o Telecomunicaciones del personal clave requerido como LIDER DEL PROYECTO Y RESPONSABLE DE LA AUDITORIA Y CUMPLIMIENTO DE LA NORMA ISO27001:2022 – EXTERNO.
- Titulado Universitario Colegiado en Computación e Informática y/o Sistemas y/o Electrónica y/o Redes y Comunicaciones y/o Telecomunicaciones del personal clave requerido como GESTOR DEL SERVICIO – EXTERNO.
- Técnico Titulado y/o bachiller y/o Universitario en Computación e Informática y/o Sistemas y/o Electrónica y/o Redes y Comunicaciones y/o Telecomunicaciones del personal clave requerido como ESPECIALISTA EN CIBERSEGURIDAD Y HACKING ÉTICO – EXTERNO.
- Bachiller y/o Titulado Universitario en Sistemas y/o Electrónica y/o Informática y/o Redes y Comunicaciones y/o similares del personal clave requerido como OPERADOR DEL SERVICIO IN-SITU.

Acreditación:

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

El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.

En caso título técnico o profesional o bachiller no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.

En caso se acredite estudios en el extranjero del personal clave, debe presentarse adicionalmente copia simple del documento de la revalidación o del reconocimiento ante SUNEDU, del grado académico o título profesional otorgados en el extranjero, según corresponda.

C.2.2 Capacitación del personal clave

Requisitos:

- Del personal clave requerido como LIDER DEL PROYECTO Y RESPONSABLE DE LA AUDITORIA Y CUMPLIMIENTO DE LA NORMA ISO27001:2022 – EXTERNO.
 - Dieciocho (18) horas lectivas, académicas y/o pedagógicas, en Taller y/o Diploma y/o Curso de formación en Gestión de la Ciberseguridad desde un enfoque corporativo, bajo los lineamientos de la ISO 27032
 - Dieciocho (18) horas lectivas, académicas y/o pedagógicas, en Taller y/o Diploma y/o Curso de formación en Gestión y Administración de la seguridad

de la información, bajo el enfoque de la norma ISO 27001.

- Del personal clave requerido como GESTOR DEL SERVICIO – EXTERNO
 - Ocho (08) horas lectivas, académicas y/o pedagógicas, en “Taller de Gestión de CIBERCRISIS”
- Del personal clave requerido como ESPECIALISTA EN CIBERSEGURIDAD Y HACKING ÉTICO – EXTERNO
 - Ocho (08) horas lectivas, académicas y/o pedagógicas, en “Taller de Gestión de CIBERCRISIS”.
 - Ciento veinte (120) horas lectivas, académicas y/o pedagógicas, en Taller y/o Curso y/o Programa de Especialización en CIBERSEGURIDAD DEFENSIVA, realizado por una institución de formación especializada.

Acreditación:

Se acreditará con copia simple de constancias, certificados, u otros documentos, según corresponda.

Advertencia

Al evaluar la incorporación de este requisito, la entidad contratante debe sustentar que el tipo de capacitación seleccionado se encuentre vinculado con las actividades que se va de desempeñar el personal clave.

Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas , según la normativa de la materia.

C.3. EQUIPAMIENTO ESTRÁTEGICO

Como parte del servicio del Cybersoc, el CONTRATISTA deberá implementar en la etapa del implementación dentro de los 30 días calendarios, posteriores a la conformidad del Plan de Trabajo, considera la provisión, instalación y puesta en operación un sistema de Video Wall de propiedad del contratista, el cual se integrará a la red corporativa; para la visualización de la operación del servicio (con todos los componentes de seguridad implementados) por parte del personal de la Gerencia de Tecnologías de la Información y comunicaciones. El sistema de video wall será implementado en la Sala GTIC Ex OACI, donde se encontrará el operador del servicio in situ. El sistema de Video Wall debe contar con su software para visualización en los monitores, el cual debe estar integrado en la red para visualizar los sistemas del Cybersoc.

Características Mínimas

Se requiere un (1) sistema de Video Wall, debe contar con al menos 04 pantallas, con sus respectivos rack y controlador de video, se instalarán en la sala destinada a la operación del servicio en edificio Ex OACI para la monitorización de los servicios del Cybersoc implementado:

Pantallas características:

- 4 und - Tamaño de pantalla 46", Tecnología LED
- Resolución mínima del Panel 1920 x 1080 (16: 9) Full HD
- Brillo de pantalla 500 cd/m2
- Relación de contraste 3500:1
- Ángulo de visión (horizontal/vertical) 178°/178°
- Orientación Paisaje/Retrato

- Tiempo de respuesta (8ms G-a-G).
- Fuente de alimentación AC 100 - 240 V ~ (+/- 10%), 50/60 Hz
- Módulo de hardware especial Wi-Fi Embedded.

Características Controlador de video:

- soportar mínimo 04 pantallas, debe ser administrable vía web, Resolución 800 x 480, 2048 x 1080 (1080p) de tipo Pared de TV independiente.
- Hardware apropiado de última generación para un de rendimiento optimizado.
- Debe contar con Puerto Ethernet para su conexión a la red corporativa.
- Debe operar con Navegadores Internet Explore, Mozilla, Chrome actualizados publicados en el mercado.
- Debe contar con Sistema operativo Embebido.
- De incluir todas sus licencias.

El equipamiento estratégico será de propiedad del contratista y operará por la duración del servicio 1095 días y al final del servicio será retirado de la corporación por el mismo contratista

Acreditación:

Copia de documentos que sustenten la propiedad, la posesión, el compromiso de compraventa o alquiler u otro documento que acredite la disponibilidad del equipamiento estratégico requerido está disponible para la ejecución del contrato.

Advertencia

En el caso que el postor sea un consorcio los documentos de acreditación de este requisito pueden estar a nombre del consorcio o de uno de sus integrantes.

CAPÍTULO IV FACTORES DE EVALUACIÓN

Los factores de evaluación son determinados por los evaluadores. En la contratación de servicios en general, la evaluación de la oferta consiste en: i) Evaluación Técnica y ii) Evaluación Económica.

La evaluación económica de la oferta es posterior a la evaluación técnica de acuerdo con el artículo 94 del Reglamento. El puntaje máximo de cada una de estas evaluaciones es equivalente a cien puntos.

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

2.1. EVALUACIÓN TÉCNICA

La evaluación técnica se realiza sobre cien puntos. Para acceder a la etapa de evaluación económica, el postor debe obtener un puntaje técnico mínimo de setenta puntos.

4.1.2. FACTORES DE EVALUACIÓN FACULTATIVOS

A. EXPERIENCIA DEL PERSONAL CLAVE	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
<p><u>Requisitos:</u></p> <p>Se evaluará en función al tiempo de experiencia del personal clave: LIDER DEL PROYECTO Y RESPONSABLE DE LA AUDITORÍA Y CUMPLIMIENTO DE LA NORMA ISO 27001:2022 – EXTERNO en Servicios de ciberseguridad y/o seguridad de la información.</p> <p><u>Acreditación:</u></p> <p>La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p> <p>Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.</p> <p>En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.</p>	<p>[Como máximo 40] puntos</p> <p>Más de 06 años: 40 puntos</p> <p>Más de 05 hasta 06 años: 35 puntos</p> <p>Más de 04 hasta 05 años: 30 puntos</p>

<p>Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco años anteriores a la fecha de la presentación de ofertas.</p> <p>De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.</p>	
--	--

B. SOSTENIBILIDAD SOCIAL	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
<p><u>Evaluación:</u></p> <p>Se evaluará que el postor cuente con una o más prácticas de sostenibilidad social.</p> <p>En caso de consorcios, los integrantes que realizan actividades relacionadas a la sostenibilidad social acreditan alguna de las prácticas, según las obligaciones que asumen en el consorcio que conforman.</p> <p><u>Prácticas:</u></p> <ul style="list-style-type: none"> Inscripción vigente en el Registro Nacional de Empresas Promocionales para Personas con Discapacidad (REPPCD) del Ministerio de Trabajo y Promoción del Empleo⁹. Reconocimiento del Ministerio de Trabajo ¹⁰ o certificación en buenas prácticas laborales vinculadas al salario justo, entornos de trabajo seguros y sin riesgos para la salud, entornos de trabajo equitativos y con igualdad de oportunidades de desarrollo humano, sistemas o políticas sobre debida diligencia para erradicar el trabajo infantil y el trabajo forzoso. Los evaluadores deberán detallar específicamente los documentos para la acreditación respectiva. Inscripción vigente en el Registro de Empresas Promocionales para Personas con Discapacidad (REPPCD) del Ministerio de Trabajo y Promoción del Empleo.¹¹ <p><u>Acreditación:</u></p> <p>Se acreditará mediante la presentación del Certificado correspondiente emitido por el Ministerio de Trabajo.</p>	<p>[Como máximo 5] puntos</p> <p>Acredita una (1) de las prácticas de sostenibilidad social. 05 puntos</p> <p>No acredita ninguna práctica en sostenibilidad social. 0 puntos</p>

⁹ De acuerdo con el Reglamento de la Ley N° 29963, Ley General de la persona con discapacidad, aprobado mediante Decreto Supremo N° 002-2014-MIMP.

¹⁰ Mediante Resolución Ministerial N° 074-2019-TR, modificada por Resolución Ministerial N° 304-2020-TR y Resolución Viceministerial N° 001-2024-MTPE/2 del Ministerio de Trabajo y Promoción del Empleo se aprueban los Lineamientos para el Otorgamiento del Reconocimiento de Buenas Prácticas Laborales.

¹¹ La inscripción en el REPPCD tiene una vigencia de doce meses, a cuyo vencimiento queda sin efecto de manera automática. Antes de su vencimiento, puede ser renovado.

C. INTEGRIDAD EN LA CONTRATACIÓN PÚBLICA	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
<p><u>Evaluación:</u></p> <p>Se evaluará que el postor cuente con certificación del sistema de gestión antisoborno</p> <p><u>Acreditación:</u></p> <p>Copia simple del certificado que acredita que se ha implementado un sistema de gestión antisoborno acorde con la norma ISO 37001:2016 o con la Norma Técnica Peruana equivalente (NTP-ISO 37001:2017).</p> <p>El certificado debe haber sido emitido por un Organismo de Certificación acreditado para dicho sistema de gestión, ya sea ante el INACAL u otro organismo acreditador que cuente con reconocimiento internacional.¹²</p> <p>El referido certificado debe corresponder a la sede, filial u oficina a cargo de la prestación¹³, y estar vigente¹⁴ a la fecha de presentación de ofertas.</p> <p>En caso de que el postor se presente en consorcio, cada uno de sus integrantes, debe acreditar que cuenta con la certificación para obtener el puntaje.</p>	<p>[Cómo máximo 5] puntos</p> <p>Presenta Certificado ISO 37001 05 puntos</p> <p>No presenta Certificado ISO 37001 0 puntos</p>

D. CAPACITACIÓN AL PERSONAL DE LA ENTIDAD CONTRATANTE	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
<p><u>Evaluación:</u></p> <p>Se evaluará en función a la oferta de capacitación a cinco (05) Profesionales Informáticos de CORPAC SA en temas relacionadas a CompTIA Security+ mediante modalidad de sesiones de plataforma virtual. El perfil del capacitador es de un Titulado en Computación e informática y/o Sistemas y/o Electrónica y/o Redes y Comunicaciones y/o Telecomunicaciones.</p> <p>El postor que oferte esta capacitación se obliga a entregar los certificados o constancias del personal capacitado a la entidad contratante.</p> <p>Advertencia</p>	<p>[Como máximo 20] puntos</p> <p>Más de 05 horas: 20 puntos</p> <p>Más de 03 horas: 15 puntos</p>

¹² Sea firmante/signatario del Acuerdo de Reconocimiento Mutuo (MLA) del International Accreditation Forum-IAF (<http://www.iaf.nu>) o del InterAmerican Accreditation Cooperation-IAAC (<http://www.iaac.org.mx>) o del European co-operation for Accreditation-EA (<http://www.european-accreditation.org/>).

¹³ En el certificado debe estar consignada la dirección exacta de la sede, filial u oficina a cargo de la prestación.

¹⁴ Se refiere al periodo de vigencia que señala el certificado presentado.

<p><i>Las calificaciones del capacitador que se pueden requerir son el grado académico de bachiller o título profesional, así como, de ser el caso, experiencia no mayor de dos años, vinculada a la materia de la capacitación relacionada con la prestación de servicios a ser contratados.</i></p>	
<p>Acreditación: Se acreditará únicamente mediante la presentación de una declaración jurada.</p>	

E. MEJORAS A LOS TÉRMINOS DE REFERENCIA	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
<p>Evaluación:</p> <p>Mejora 1:</p> <p>Un (01) ejercicio adicional de hacking ético con remediación integral asistida al año, adicional a lo establecido en los Términos de Referencia, sin costo alguno para CORPAC S.A.</p> <p>Mejora 2:</p> <p>Cobertura adicional del 10% en el servicio de prevención, detección, análisis, investigación y respuesta ante incidentes de ciberseguridad, aplicable a servidores y estaciones de trabajo a nivel nacional, adicional a lo establecido en los Términos de Referencia, sin costo alguno para CORPAC S.A.</p> <p>Acreditación: Se acreditará únicamente mediante la presentación de Declaración Jurada.</p>	<p>[Como máximo 20] puntos</p> <p>Mejora 1 : 10 puntos</p> <p>Mejora 2 : 10 puntos</p>
<p>Advertencia</p> <p><i>Constituye una mejora, todo aquello que agregue un valor adicional al parámetro mínimo establecido en el requerimiento, según corresponda, mejorando su calidad o las condiciones de su entrega o prestación, sin generar un costo adicional a la entidad contratante.</i></p>	

F. SISTEMA DE GESTIÓN DE LA CALIDAD	PUNTAJE / METODOLOGÍA PARA SU ASIGNACIÓN
<p>Evaluación:</p> <p>Se evalúa que el postor cuente con un sistema de gestión de la</p>	<p>[Como máximo 10] puntos</p> <p>Presenta Certificado ISO 9001:2015: 10 puntos</p> <p>No presenta Certificado ISO 9001:2015: 0 puntos</p>

<p>calidad certificado¹⁵ acorde con ISO 9001:2015¹⁶ o Norma Técnica Peruana equivalente (NTP-ISO 9001:2015), cuyo alcance o campo de aplicación del certificado considere el servicio de monitoreo y alerta de seguridad CYBERSOC¹⁷.</p> <p><u>Acreditación:</u> Mediante la presentación de copia simple de certificado oficial emitido por un Organismo de Certificación acreditado para dicho Sistema de Gestión, ya sea ante el INACAL (antes INDECOPI) u otro organismo acreditador que cuente con reconocimiento internacional¹⁸. El referido certificado debe estar a nombre del postor¹⁹ y corresponder a la sede, filial u oficina a cargo de la prestación²⁰, y estar vigente²¹ a la fecha de presentación de ofertas.</p> <p>En caso de que el postor se presente en consorcio, cada uno los integrantes que vaya a ejecutar las actividades relacionadas al alcance del certificado, debe acreditar que cuenta con la certificación para obtener el puntaje.</p>	
---	--

CUADRO RESUMEN FACTORES DE EVALUACIÓN

FACTORES DE EVALUACIÓN FACULTATIVOS	PUNTAJE
A. EXPERIENCIA DEL PERSONAL CLAVE	[MÁXIMO 40] puntos / NO CORRESPONDE
B. SOSTENIBILIDAD SOCIAL	[MÁXIMO 5] puntos / NO CORRESPONDE
C. INTEGRIDAD EN LA CONTRATACIÓN PÚBLICA	[MÁXIMO 5] puntos / NO CORRESPONDE
D. CAPACITACIÓN AL PERSONAL DE LA ENTIDAD CONTRATANTE	[MÁXIMO 20] puntos / NO CORRESPONDE
E. MEJORAS A LOS TÉRMINOS DE REFERENCIA	[MÁXIMO 20] puntos / NO CORRESPONDE

¹⁵ La Certificación implica que un organismo de certificación independiente garantiza la conformidad de los productos/ servicios/procesos o sistemas de una organización, frente a los requisitos de una norma establecida.

¹⁶ Entre las certificaciones más difundidas mundialmente, y que es aplicable a todas las organizaciones independientemente de su actividad o sector, referidas a la implementación de un sistema de gestión de la calidad, se encuentra la correspondiente a la norma internacional ISO 9001, propuesto por la Organización Internacional para la Estandarización (ISO). La certificación de la norma ISO 9001 confirma que una organización ha demostrado mediante una evaluación (Auditoría de Tercera Parte) la implementación de un Sistema de Gestión de la Calidad, y con ello su capacidad para proporcionar regularmente productos o servicios que satisfagan los requisitos de esa Norma Internacional, del cliente y los legales y reglamentarios aplicables, así como su compromiso por aumentar la satisfacción del cliente a través de la aplicación eficaz y mejora continua del sistema.

¹⁷ Respecto de la definición del alcance o campo de aplicación del certificado, en función al objeto de contratación, se describe a manera de ejemplo, el caso de la contratación del servicios de limpieza (donde además, por la particularidad del servicio, es importante tomar en cuenta el ámbito geográfico), donde se pueden considerar términos como: "limpieza de instalaciones en la ciudad de...", "limpieza de centros educativos en las ciudades de...", "limpieza de edificaciones en la provincia de...", "limpieza de ambientes hospitalarios en el departamento de...", "limpieza de centros educativos en la Región de...", "limpieza de instalaciones a nivel nacional", entre otros.

¹⁸ Sea firmante del Acuerdo de Reconocimiento Mutuo de ILAC (International Accreditation Cooperation) o del IAAC (Inter American Accreditation Cooperation).

¹⁹ En caso de que el postor se presente en consorcio, para obtener el puntaje respectivo, todos sus integrantes deben acreditar que cuentan con las certificaciones vigentes con el alcance requerido, siempre que, de acuerdo con la promesa de consorcio, se hubieran comprometido a ejecutar obligaciones vinculadas directamente al objeto de la convocatoria.

²⁰ En el certificado debe estar consignada la dirección exacta de la sede, filial u oficina a cargo de la prestación.

²¹ Se refiere al periodo de vigencia que señala el certificado presentado.

F. SISTEMAS DE GESTIÓN DE CALIDAD	[MÁXIMO 10] puntos / NO CORRESPONDE
PUNTAJE TOTAL	100 puntos ²²

2.2. EVALUACIÓN ECONÓMICA (Puntaje Máximo: 100 Puntos)

OFERTA ECONÓMICA	PUNTAJE/METODOLOGÍA PARA SU ASIGNACIÓN
<p><u>Evaluación:</u></p> <p>Se evalúa considerando el precio ofertado por el postor.</p> <p><u>Acreditación:</u></p> <p>Se acredita mediante el documento que contiene el precio de la oferta (Anexo N° 6).</p>	<p>La evaluación consiste en otorgar el mayor puntaje a la oferta del menor monto ofertado y otorgar a las demás ofertas puntajes inversamente proporcionales a sus respectivos montos ofertados, según la siguiente fórmula:</p> $Po = \frac{Mb \times Pmax}{Mo}$ <p>Po = Puntaje de la oferta económica a evaluar Mo = Monto de la oferta económica Mb = Monto de la oferta económica más baja Pmax = Puntaje máximo</p> <p style="text-align: right;">100²³ puntos</p>

2.3. PUNTAJE TOTAL

El puntaje total de las ofertas es el promedio ponderado de la evaluación técnica y la evaluación económica, aplicándose la siguiente fórmula:

$$PTP = c_1 PT + c_2 Pe$$

Donde:

PTP	=	Puntaje total del postor a evaluar
Pt	=	Puntaje de la evaluación técnica del postor a evaluar
Pe	=	Puntaje de la evaluación económica del postor a evaluar
c1	=	Coeficiente de ponderación para la evaluación técnica: 0.60
c2	=	Coeficiente de ponderación para la evaluación económica: 0.40

Donde: 0.60 + 0.40 = 1.00

²² Es la suma de los puntajes de todos los factores de evaluación.

²³ De acuerdo con lo señalado en el numeral 75.2 del artículo 75 del Reglamento.

CAPÍTULO V PROFORMA DEL CONTRATO

Advertencia

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

Conste por el presente documento, la contratación de **SERVICIO DE MONITOREO Y ALERTA DE SEGURIDAD - CYBERSOC**, que celebra de una parte **CORPORACIÓN PERUANA DE AEROPUERTOS Y AVIACION COMERCIAL S.A.**, en adelante LA ENTIDAD CONTRATANTE, con RUC N°20100004675, con domicilio legal en **AV. ELMER FAUCETT NRO. 3400 (ANTIGUO ARPTO INTERNACIONAL JORGE CHAVEZ) PROV. CONST. DEL CALLAO**, 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 [.....], los evaluadores adjudicaron la buena pro de la **CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC S.A.- PRIMERA CONVOCATORIA** para la contratación de **SERVICIO DE MONITOREO Y ALERTA DE SEGURIDAD - CYBERSOC**, 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 **CONTRATACIÓN SERVICIO DE MONITOREO Y ALERTA DE SEGURIDAD - CYBERSOC**.

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 total del servicio, incluyendo, de ser aplicable, todos los impuestos, 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 PAGO²⁴

LA ENTIDAD CONTRATANTE se obliga a pagar la contraprestación a EL CONTRATISTA en **SOLES**, en **PAGOS MENSUALES**, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas aprobado por Decreto Supremo N° 009-2025-EF.

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 del día siguiente de recibido el entregable, 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 veinte (20) días, bajo responsabilidad de dicho servidor.

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

LA ENTIDAD CONTRATANTE debe efectuar el pago dentro de los diez (10) días hábiles siguientes de otorgada la conformidad de los servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del servidor competente.

En caso de retraso en el pago por parte de LA ENTIDAD CONTRATANTE, 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 67 de la Ley N° 32069, Ley General de Contrataciones Públicas.

Importante para la entidad contratante

- En caso de que la ENTIDAD CONTRATANTE verifique en la Pladicop que el CONTRATISTA tiene multas impagas que no se encuentren en procedimiento coactivo, se debe incluir la siguiente cláusula:

CLÁUSULA [...]: COMPROMISO DE PAGO DE MULTA

Durante la ejecución del contrato la ENTIDAD CONTRATANTE retiene al CONTRATISTA de forma prorrateada desde el primer o único pago que se realice, según corresponda, hasta el 10% del monto del contrato, para el pago o amortización de multas impagas impuestas en el marco de lo previsto en el artículo 89 de la Ley N° 32069, que no se encuentran en procedimiento coactivo.

- En el caso que, adicionalmente, el proveedor presente la DECLARACIÓN JURADA SOBRE INAPLICACIÓN DEL IMPEDIMENTO TIPO 4.D DEL INCISO 4 DEL NUMERAL 30.1 DEL ARTÍCULO 30 DE LA LEY N° 32069 REFERIDO A LA INSCRIPCIÓN EN EL REGISTRO DE DEUDORES ALIMENTARIOS MOROSOS – REDAM que autoriza descuento para el pago de deuda alimentaria, se debe indicar la siguiente cláusula:

CLÁUSULA : AUTORIZACIÓN DE DESCUENTO DE PENSIÓN ALIMENTARIA

EL CONTRATISTA autoriza que se le descuenta del pago de su contraprestación el monto de la pensión mensual fijada en el proceso de alimentos ascendiente a [CONSIGNAR MONTO] seguido por [CONSIGNAR LOS DATOS DE LA PARTE DEMANDANTE DEL PROCESO DE ALIMENTOS] ante el [CONSIGNAR LOS DATOS DE IDENTIFICACIÓN DEL JUZGADO CORRESPONDIENTE] en el trámite del expediente [CONSIGNAR EL NÚMERO DE EXPEDIENTE JUDICIAL].

CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN

El plazo de ejecución del presente contrato es de [...], el mismo que se computa desde [CONSIGNAR SI ES DESDE EL DÍA SIGUIENTE DEL PERFECCIONAMIENTO DEL CONTRATO O DESDE LA NOTIFICACIÓN DE LA ORDEN DE SERVICIO O DESDE LA FECHA QUE SE ESTABLEZCA EN EL CONTRATO O DESDE LA FECHA EN QUE SE CUMPLAN LAS CONDICIONES PREVISTAS EN EL CONTRATO PARA EL INICIO DE LA EJECUCIÓN, DEBIENDO INDICAR LAS MISMAS EN ESTE ULTIMO CASO.]

Importante para la entidad contratante

En caso de contratos de contingencia utilizados de acuerdo con el artículo 285 del Reglamento se incluyen obligatoriamente las siguientes cláusulas:

CLÁUSULA [...]: CONDICIÓN O EVENTO QUE ACTIVA LA EJECUCIÓN DEL CONTRATO

La activación de la ejecución del contrato se produce cuando [CONSIGNAR EL EVENTO FUTURO E INCIERTO QUE CONDICIONA LA EJECUCIÓN DEL CONTRATO, DE ACUERDO CON EL ARTÍCULO 284 DEL REGLAMENTO]

CLÁUSULA [...]: MECANISMOS DE ACTIVACIÓN (PROTOCOLO), CONTROL, SEGUIMIENTO Y EVALUACIÓN

Los mecanismos de activación (protocolo), control, seguimiento y evaluación de la ejecución contractual son [CONSIGNAR LOS REFERIDOS MECANISMOS CONFORME LO SEÑALADO EN EL REQUERIMIENTO Y LA OFERTA GANADORA]

En caso de contratos de contingencia en los que se aplique la modalidad de pago "pago por disponibilidad" de acuerdo con el artículo 285 del Reglamento, se incluye obligatoriamente la siguiente cláusula:

CLÁUSULA [...]: CONDICIONES DE AMPLIACIÓN DE PLAZO DEL CONTRATO

Al culminar el plazo del contrato sin que se haya activado la ejecución del contrato, las partes acuerdan las siguientes condiciones para ampliar el plazo contractual por un periodo adicional: [CONSIGNAR LAS CONDICIONES ACORDADAS]

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

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, incluyendo las modificaciones contractuales y adendas aprobadas por la entidad contratante, de ser el caso.

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 CONTRATANTE, por los conceptos, montos y vigencias siguientes:

Garantía de fiel cumplimiento del contrato: Por la suma de [CONSIGNAR EL MONTO], a través de la [INDICAR EL MECANISMO DE GARANTÍA PRESENTADO: CONTRATO DE SEGURO/CARTA FIANZA FINANCIERA/RETENCIÓN DE PAGO/DECLARACIÓN JURADA DE CONSTITUCIÓN DE FIDEICOMISO] N° [INDICAR NÚMERO DEL DOCUMENTO] emitida por [SEÑALAR EMPRESA QUE LA EMITE], la misma que debe mantenerse vigente hasta la conformidad de la conformidad de la prestación. El monto señalado es equivalente al diez por ciento (10%) del monto del contrato original.

CLÁUSULA OCTAVA: EJECUCIÓN DE GARANTÍAS POR FALTA DE RENOVACIÓN

LA ENTIDAD CONTRATANTE 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 artículo 118 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

CLÁUSULA NOVENA: CONFORMIDAD DE LA PRESTACIÓN

La conformidad de la prestación se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley 32069, Ley General de Contrataciones Públicas. La conformidad es otorgada por el Área de Redes, Comunicaciones y Soporte Técnico y la Gerencia de Tecnología de la Información y comunicaciones de CORPAC en el plazo máximo de siete (7) días computados desde el día siguiente de producida la recepción.

De existir observaciones, LA ENTIDAD CONTRATANTE las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar, el cual no debe ser mayor al 30% del plazo del entregable²⁵ correspondiente, dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. Si pese al plazo otorgado, EL CONTRATISTA no cumpliera a cabalidad con la subsanación, LA ENTIDAD CONTRATANTE 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 sin considerar los días en los que pudiera incurrir la entidad contratante para efectuar las revisiones y notificar las observaciones correspondientes.

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

²⁵ En caso de que el plazo obtenido como resultado de la aplicación del porcentaje sea una cifra decimal, corresponde que la entidad contratante efectúe el redondeo a favor del contratista, computándose como un día completo adicional en dicho supuesto.

CLÁUSULA DÉCIMA: GESTIÓN DE RIESGOS

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

CLÁUSULA UNDÉCIMA: RESPONSABILIDAD POR VICIOS OCULTOS

La recepción conforme de la prestación por parte de LA ENTIDAD CONTRATANTE no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 69 de la Ley N° 32069, Ley General de Contrataciones Públicas y el artículo 144 de su Reglamento.

El plazo máximo de responsabilidad del contratista es de tres (03) año(s) contado a partir de la conformidad otorgada por LA ENTIDAD CONTRATANTE.

CLÁUSULA DUODÉCIMA TERCERA: PENALIDADES

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

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

Donde:

F = 0.40

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 CONTRATANTE no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme al numeral 120.4 del artículo 120 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

OTRAS PENALIDADES

Otras Penalidades			
N°	Supuestos de aplicación de penalidad	Forma de cálculo	Procedimiento
1	Realizar cambios de personal asignado al servicio, sin contar con la aprobación de la Gerencia de Tecnología de la Información y Comunicaciones	10% de la UIT. Se aplicará la penalidad por cada ocurrencia	Mediante informe de la Gerencia de Tecnología de la Información y Comunicaciones, la cual supervisará el servicio.

Por incumplimientos de Niveles de Servicio (SLA)

Penalidades en SERVICIOS DE CYBERSOC		
Servicio	SLA	Penalidad
		Superar los 30 minutos de indisponibilidad del servicio,

Monitoreo de salud de la plataforma	Disponibilidad diaria 24x7x365	por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.			
Monitoreo avanzado tiempo real y correlación de eventos de seguridad	Disponibilidad diaria 24x7x365	Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.			
Cyber Threat Intelligence (Inteligencia de Ciberseguridad)	Disponibilidad diaria 24x7x365	Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.			
Threat Hunting	Disponibilidad diaria 24x7x365	Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.			
Alerta Temprana	Disponibilidad diaria 24x7x365	Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.			
Portal de Supervisión	Disponibilidad diaria 24x7x365	Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.			
Penalidades en Advanced Security Incident Response (Respuesta Avanzada a Incidentes)					
Registro de incidente: Ticket generado por	Tiempo promedio de detección e inicio del	Tiempo promedio de	Tiempo promedio de reparación	Tiempo promedio de resolución	Análisis de

CONTRATISTA	análisis	contenci ón			repercus iones
<= 15 minutos de reportado el incidente	< 30 minutos	< 45 minutos	< 3 horas	< 6 horas	Dentro de las 48 horas de resuelto el incidente.
Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	Penalidad : 3% de UIT por cada ocurrenci a de incumplim iento	Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	Penalida d: 3% de UIT por cada ocurrenci a de incumpli miento
Penalizaciones por Tiempos de Atención Off-Site					
Disponibilidad 24 x 7 x 365			Superar los 30 minutos de indisponibilidad del servicio, por cada evento reportado: 3% de la UIT Se aplicará la penalidad por cada ocurrencia y se reportará en cada ciclo mensual.		
2 horas de atención como plazo máximo en Lima Metropolitana			Penalidad: 3% de UIT por cada ocurrencia de incumplimiento		
4 horas de atención como plazo máximo en provincias			Penalidad: 3% de UIT por cada ocurrencia de incumplimiento		
Penalizaciones por Registro de tickets de mesa de ayuda					
Tiempo máximo de registro del incidente, desde que son reportados		15 minutos		Penalidad: 3% de UIT por cada ocurrencia de incumplimiento	

La suma de la aplicación de estos dos tipos de penalidades no debe exceder el 10% del monto vigente del contrato, o de ser el caso, del ítem correspondiente.

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

Cuando se llegue a cubrir el monto máximo de la aplicación de la penalidad por mora y otras penalidades, de ser el caso, LA ENTIDAD CONTRATANTE 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 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas.

De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES proceden de acuerdo a lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

Importante para la entidad contratante

- Sólo en el caso que la entidad contratante hubiese previsto durante la estrategia de contratación, la aplicación de la figura de resolución por terminación anticipada se debe incluir la siguiente cláusula:

CLÁUSULA [...]: RESOLUCIÓN POR TERMINACIÓN ANTICIPADA

Las partes acuerdan la resolución por terminación anticipada del contrato cuando el resultado de algún hito impida o haga innecesaria la continuidad del siguiente, sin que resulte atribuible a alguna de las partes, de acuerdo con lo previsto en el artículo 121 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas.

Los hitos del contrato son [INCLUIR EL DETALLE DE LOS HITOS DEL CONTRATO]

- Para el caso de contratos de contingencia con modalidad de pago por disponibilidad se incluye la siguiente cláusula:

“CLÁUSULA [...]: RESOLUCIÓN POR TERMINACIÓN ANTICIPADA

Las partes acuerdan la resolución por terminación anticipada del contrato en caso la entidad verifique que el contratista incumple con mantener [INDICAR EL INCUMPLIMIENTO DETERMINADO EN LOS TERMINOS DE REFERENCIA, YA SEA LA ROTACIÓN, STOCK O CAPACIDAD DE RESPUESTA, SEGÚN CORRESPONDA AL OBJETO CONTRACTUAL]”,

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

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 Y ANTISOBORNO

A la suscripción de este contrato, EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante.

Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación²⁶ y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios,

²⁶ Artículo 9 de la Ley N°32069, Ley General de Contrataciones Públicas.

asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato²⁷. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco²⁸. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar²⁹.

CLÁUSULA DÉCIMA SEXTA: MARCO LEGAL DEL CONTRATO

El marco legal comprende la Ley N° 32069, Ley General de Contrataciones Públicas y su Reglamento aprobado por Decreto Supremo N° 009-2025-EF, las directivas que emita la Dirección General de Abastecimiento del Ministerio de Economía y Finanzas, así como el OECE y demás normativa especial que resulte aplicable.

CLÁUSULA DÉCIMA SÉTIMA: SOLUCIÓN DE CONTROVERSIAS³⁰

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

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

El Laudo arbitral emitido es inapelable, definitivo y obligatorio para las partes desde el momento de su notificación, según lo previsto en el numeral 84.9 del artículo 84 de la Ley General de Contrataciones Públicas.

CLÁUSULA DÉCIMA OCTAVA: CONVENIO ARBITRAL

Las partes acuerdan que todo litigio y controversia resultante de este contrato o relativo a éste, se resolverá mediante arbitraje de acuerdo con los artículos 332 y 333 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF. El arbitraje es organizado y administrado por **[CONSIGNAR LA INSTITUCIÓN ARBITRAL, CORTE ARBITRAL CONSTITUIDA EN OTRO PAÍS O UN FORO DE REPUTACIÓN RECONOCIDA INTERNACIONALMENTE, SEGÚN CORRESPONDA]** de conformidad con sus reglamentos y estatutos vigentes, a los cuales las partes se someten libremente y considerando **[INDICAR LAS ESTIPULACIONES ADICIONALES QUE LAS PARTES HAYAN ACORDADO SEGÚN EL NUMERAL 332.3 DEL ARTÍCULO 332 DEL REGLAMENTO DE LA LEY N° 32069, LEY GENERAL DE CONTRATACIONES PÚBLICAS, APROBADO POR DECRETO SUPREMO N° 009-2025-EF]**

Advertencia

La Institución Arbitral es elegida por el postor ganador de la buena pro de la lista de instituciones arbitrales que haya propuesto la entidad contratante en las bases del procedimiento de selección. Para dicho efecto, al remitir los documentos para la suscripción del contrato, el postor ganador de la buena pro comunica la Institución Arbitral elegida de la referida lista, caso contrario, acuerda con la entidad

²⁷ Literal d) del Numeral 68.1 del Artículo 68 de la Ley N°32069, Ley General de Contrataciones Públicas.

²⁸ Literal d) del artículo 274 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas

²⁹ Numeral 122.6 del artículo 122 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas.

³⁰ De acuerdo con el numeral 84.1 del artículo 84 de la Ley General de Contrataciones Públicas, las partes pueden recurrir al arbitraje ad hoc solo cuando el monto de la controversia no supere las diez UIT.

contratante una Institución Arbitral distinta. En caso de falta de acuerdo, la Institución Arbitral es elegida de la mencionada lista por la entidad contratante de manera definitiva.

Las partes pueden establecer estipulaciones adicionales o modificatorias del convenio arbitral, en la medida que no contravengan las disposiciones de la normativa de contrataciones públicas y/o las disposiciones especiales contenidas en la normativa general de arbitraje.

El arbitraje es resuelto por árbitro único o por un tribunal arbitral conformado por tres árbitros, según el acuerdo de las partes, conforme a lo dispuesto en numeral 84.2 del artículo 84 de la Ley. En caso de duda o falta de acuerdo, el arbitraje es resuelto por árbitro único, a no ser que la complejidad o cuantía de las controversias justifique la conformación de un tribunal arbitral, lo cual es determinado por las partes o conforme al Reglamento de la institución arbitral competente. En el caso de los arbitrajes ad hoc, la controversia es resuelta por árbitro único.

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: NOTIFICACIONES DURANTE LA EJECUCIÓN CONTRACTUAL

Las partes declaran el siguiente domicilio para efecto de las notificaciones que se realicen vía notarial conforme la Décimo Tercera Disposición Complementaria Transitoria del Reglamento:

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

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 días calendario.

El CONTRATISTA señala el siguiente correo electrónico para efectos de las notificaciones que se realicen durante la ejecución del presente contrato, que no se realicen a través del SEACE de la Pladipoc:

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

La variación del correo electrónico aquí declarado debe ser comunicada a la entidad contratante, formalmente y por escrito, con una anticipación no menor de cinco 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 CONTRATANTE”

“EL CONTRATISTA”

Advertencia

La entidad contratante suscribe el contrato mediante firma digital, en caso de que el postor adjudicado con la buena pro cuente con certificado digital emitido por una entidad de certificación, de acuerdo con la normativa de la materia. Excepcionalmente, la entidad contratante con el debido sustento puede proceder a la firma del contrato mediante medios manuales, de acuerdo con el numeral 87.3 del artículo 87 del Reglamento,

ANEXOS

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR

Señores

EVALUADOR

CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC 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]** N° **[CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD]**, con poder inscrito en la localidad de **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]** en la Ficha N° **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]** Asiento N° **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]**, **DECLARO BAJO JURAMENTO** que la siguiente información se sujeta a la verdad:

Nombre, Denominación o Razón Social:			
Domicilio Legal:			
RUC:	Teléfono(s):		
MYPE	SI ()	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 negociación regulado en el artículo 132 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.
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 91 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicio, de ser el caso.

Asimismo, me comprometo a remitir la confirmación de recepción del correo electrónico, en el plazo máximo de dos días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, nombres y apellidos del postor o representante legal, según corresponda

Advertencia

La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la entidad contratante reciba el acuse de recepción.

Advertencia

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

ANEXO N° 1

DECLARACIÓN JURADA DE DATOS DEL POSTOR EN CONSORCIO

Señores

EVALUADORES

CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC 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 ³¹	SI ()		NO ()
Correo electrónico:			

Datos del consorciado 2			
Nombre, Denominación o Razón Social:			
Domicilio Legal:			
RUC:	Teléfono(s) :		
MYPE ³²	SI ()		NO ()
Correo electrónico:			

Datos del consorciado 3			
Nombre, Denominación o Razón Social:			
Domicilio Legal:			
RUC:	Teléfono(s) :		
MYPE ³³	SI ()		NO ()
Correo electrónico:			

Autorización de notificación por correo electrónico:

Correo electrónico común 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.

³¹ Esta información será verificada por la entidad contratante 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 artículo 114, del Reglamento. Para dicho efecto, todos los integrantes del consorcio deben acreditar la condición de micro o pequeña empresa.

³² Ibídem

³³ Ibídem

2. Solicitud de negociación regulado en el artículo 132 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.
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 91 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.
5. Respuesta a la solicitud de acceso al expediente de contratación.
6. Notificación de la orden de servicio, de ser el caso.

Asimismo, me comprometo a remitir la confirmación de recepción del correo electrónico, en el plazo máximo de dos días hábiles de recibida la comunicación.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, nombres y apellidos del representante
común del consorcio**

Advertencia

La notificación dirigida a la dirección de correo electrónico consignada se entenderá válidamente efectuada cuando la entidad contratante reciba el acuse de recepción.

ANEXO N° 2

PACTO DE INTEGRIDAD³⁴

Señores

EVALUADORES

CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC S.A.-PRIMERA CONVOCATORIA

Presente.-

El que suscribe, [...], postor y/o representante legal de **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]**, identificado con **[CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD]**, con poder inscrito en la Sede Registral de **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]** en la Ficha N° **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]** Asiento N° **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]**, en su calidad de proveedor en el ámbito de aplicación de la normativa de contratación pública, **suscribo el presente Pacto de Integridad** bajo los siguientes términos y condiciones:

PRIMERO: Declaro, bajo juramento:

1. Que conozco los impedimentos para ser participante, postor, contratista o subcontratista, establecidos en el artículo 30 de la Ley N° 32069, Ley General de Contrataciones Públicas.
2. Que los recursos que componen mi patrimonio o el patrimonio de la persona jurídica a la que represento no provienen de lavado de activos, narcotráfico, minería ilegal, financiamiento del terrorismo, y/o de cualquier actividad ilícita.
3. Que conozco la obligación de denunciar cualquier acto de corrupción cometido por los actores del proceso de contratación, así como las medidas de protección que le asisten a los denunciantes³⁵; además de las consecuencias administrativas y legales que de estos se derivan.
4. Que conozco el alcance de la Ley N° 28024, Ley que regula la gestión de intereses en la administración pública y su reglamento, aprobado por Decreto Supremo N° 120-2019-PCM, así como el marco de aplicación de la Ley N° 31564, Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público, y su reglamento aprobado por Decreto Supremo N° 082-2023-PCM³⁶.
5. Que conozco el alcance de la cláusula anticorrupción y antisoborno de los contratos suscritos en el marco del proceso de contratación y las consecuencias derivadas de su incumplimiento³⁷.

SEGUNDO: Dentro de ese marco, asumo los siguientes compromisos:

³⁴ De conformidad con el literal b del numeral 69.1 del artículo 69 y el numeral 57 del Anexo I Definiciones del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

³⁵ Decreto Legislativo N° 1327, Decreto Legislativo que establece medidas de protección para el denunciante de actos de corrupción y sanciona las denuncias realizadas de mala fe, y su Reglamento aprobado por Decreto Supremo N° 010-2017-JUS, modificado por Decreto Supremo N° 002-2020-JUS, en concordancia con la Directiva N° 002-2023-PCM-SIP: Directiva para la gestión de denuncias y solicitudes de medidas de protección al denunciante de actos de corrupción recibidas a través de la plataforma digital única de denuncias del ciudadano, aprobada por Resolución de Secretaría de Integridad Pública N° 005-2023-PCM-SIP.

³⁶ Reglamento del Ley N° 31564:

Artículo 24.- Inhabilitación de ex funcionarios, ex servidores públicos, empresas e instituciones privadas

El incumplimiento de los impedimentos señalados en el numeral 4.2 del artículo 4 de la Ley por parte de las personas, las empresas e instituciones privadas involucradas en dicho incumplimiento, es sancionado con la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad, sin perjuicio de las acciones civiles y penales a que hubiera lugar conforme al numeral 7.7 del artículo 7 de la Ley. En caso de ex funcionarios y ex servidores públicos se aplica el procedimiento administrativo disciplinario sujeto a la Ley N° 30057, Ley del Servicio Civil o normas específicas. (...)

³⁷ Conforme a lo establecido en el artículo 68 de la Ley General de Contrataciones Públicas, así como en el artículo 274 numeral d), de su Reglamento:

Artículo 68. Resolución del contrato

68.1. Cualquiera de las partes puede resolver, total o parcialmente, el contrato en los siguientes supuestos:

d) Por incumplimiento de la cláusula anticorrupción.

Artículo 274. Causales de exclusión de proveedores adjudicatarios de los catálogos electrónicos de acuerdo marco

Un proveedor adjudicatario es excluido de los Catálogos Electrónicos de Acuerdo Marco, en los siguientes casos:

d) Por incumplimiento de la cláusula anticorrupción y antisoborno.

1. Mantener una conducta proba e íntegra en todas las actividades del proceso de contratación, lo que supone actuar con honestidad y veracidad, sin cometer actos ilícitos, directa o indirectamente, así como respetar la libertad de concurrencia y las condiciones de competencia efectiva en el proceso de contratación y abstenerme de realizar prácticas que la restrinjan o afecten.

[Solo para personas jurídicas] Lo anterior se hace extensivo, para conocimiento, a los socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a la persona jurídica que represento.

2. Abstenerme de ofrecer, dar o prometer regalos, cortesías, invitaciones, donativos u otros beneficios similares, a funcionarios o servidores públicos de la dependencia encargada de las contrataciones, actores del proceso de contratación y personal de la entidad contratante.
3. Denunciar ante las autoridades competentes, de manera oportuna, los actos de corrupción, conducta funcional, conflicto de intereses u otro de naturaleza similar, respecto de lo cual tuviera conocimiento en el marco del proceso de contratación (<https://denuncias.servicios.gob.pe/>).
4. Facilitar las acciones o mecanismos implementados por la entidad pública responsable del proceso de contratación para fortalecer la transparencia, promover la lucha contra la corrupción y fomentar la rendición de cuentas.

TERCERO: Este pacto de integridad tiene vigencia desde el momento de su suscripción hasta la culminación de la fase de selección³⁸; y, en caso de resultar adjudicado con la buena pro, este mantiene su vigencia hasta la culminación del contrato.

CUARTO: Para efectos de salvaguardar el contenido del Pacto de Integridad frente a eventuales incumplimientos de los compromisos asumidos, me someto a las acciones de debida diligencia, supervisión, fiscalización posterior, iniciativas de veeduría autorizadas por la entidad contratante u otros que correspondan; así como a las responsabilidades administrativas, civiles y/o penales que se deriven de estos, conforme al marco legal vigente.

En señal de conformidad, suscribo el presente pacto de integridad, a los () días del mes () de 20(), manifestando que la información declarada se sujeta al principio de presunción de veracidad, conforme a lo dispuesto en el artículo IV del Título Preliminar de la Ley N° 27444, Ley del Procedimiento Administrativo General³⁹.

N° de DNI: Firma

³⁸ **Artículo 92. Culminación de la fase de selección**, del Decreto Supremo N°009-2025-EF:

La fase de selección culmina cuando: a) Se perfecciona el contrato, b) Se cancela el procedimiento de selección, c) Se deja sin efecto el otorgamiento de la buena pro por causa imputable a la entidad contratante, d) No se perfeccione el contrato por los supuestos establecidos en el artículo 91.

³⁹ **1.7 Principio de Presunción de Veracidad.** - En la tramitación del procedimiento administrativo, se presume que los documentos y declaraciones formulados por los administrados en la forma prescrita por esta Ley, responden a la verdad de los hechos que ellos afirman. Esta presunción admite prueba en contrario.

ANEXO N° 3⁴⁰

DECLARACIÓN JURADA

Señores

EVALUADORES

CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC 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 tener impedimento para postular en el procedimiento de selección ni para contratar con el Estado, conforme al artículo 30 de la Ley N° 32069, Ley General de Contrataciones Públicas.
- ii. Conocer las sanciones contenidas en la Ley N° 32069, Ley General de Contrataciones Públicas y su Reglamento, aprobado mediante Decreto Supremo N° 009-2025-EF, así como las disposiciones aplicables de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- iii. Participar en el presente proceso de contratación en forma independiente sin mediar consulta, comunicación, acuerdo, arreglo o convenio con ningún proveedor; y, conocer las disposiciones del Decreto Legislativo N° 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas.
- iv. Conocer, aceptar y someterme a las bases, condiciones y reglas del procedimiento de selección.
- v. Ser responsable de la veracidad de los documentos e información que presento en el presente procedimiento de selección.
- vi. 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

Advertencia

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

⁴⁰ Artículo 69 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

ANEXO N° 4

PROMESA DE CONSORCIO

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

Señores

EVALUADORES

CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC 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 **CONCURSO PÚBLICO DE SERVICIOS N° [CONSIGNAR NOMENCLATURA DEL PROCEDIMIENTO DE SELECCIÓN]**.

Asimismo, en caso de obtener la buena pro, nos comprometemos a formalizar el contrato de consorcio, de conformidad con lo establecido por los artículos 88 y 89 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas aprobado mediante Decreto Supremo N° 009-2025-EF, 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 [.....] y nuestro correo electrónico común: [.....], al cual se notificarán todas las comunicaciones dirigidas al Consorcio durante el procedimiento de selección hasta la suscripción del contrato.

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]** [%]⁴¹

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 1]

2. OBLIGACIONES DE **[NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DEL CONSORCIADO 2]** [%]⁴²

[DESCRIBIR LAS OBLIGACIONES DEL CONSORCIADO 2]

⁴¹ Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

⁴² Consignar únicamente el porcentaje total de las obligaciones, el cual debe ser expresado en número entero, sin decimales.

TOTAL OBLIGACIONES

100%⁴³

[CONSIGNAR CIUDAD Y FECHA]

.....
Consortiado 1
Nombres, apellidos y firma del consorciado 1
o de su representante legal
tipo y N° de documento de identidad

.....
Consortiado 2
Nombres, apellidos y firma del consorciado 2
o de su representante legal
tipo y N° de documento de identidad

.....
Consortiado 3
Nombres, apellidos y firma del consorciado 3
o de su Representante Legal
Tipo y N° de Documento de Identidad

⁴³ Este porcentaje corresponde a la sumatoria de los porcentajes de las obligaciones de cada uno de los integrantes del consorcio.

Advertencia

El Anexo N° 5 únicamente es presentado por los postores que, si bien son parientes de los impedidos referidos en el inciso 1 del numeral 30.1 del artículo 30 de la Ley N° 32069, Ley General de Contrataciones Públicas, no le son aplicables los impedimentos en razón de parentesco del inciso 2 del citado numeral, debido a que cumplen alguna de las siguientes condiciones: i) Han suscrito un contrato derivado de un procedimiento de selección competitivo o no competitivo o, ii) han ejecutado cuatro contratos menores en el mismo tipo de objeto al que postula. Para el caso de servicios, los dos años son consecutivos.

ANEXO N° 5⁴⁴
DECLARACIÓN JURADA DE DESAFECTACIÓN DE IMPEDIMENTO

Señores

EVALUADORES

CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC S.A.-PRIMERA CONVOCATORIA

Presente.-

El que suscribe, [...], postor y/o representante legal de **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]**, identificado con **[CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD]**, con poder inscrito en la Sede Registral de **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]** en la Ficha N° **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]** Asiento N° **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]**, **declaro que tengo los siguientes parientes⁴⁵, los cuales cuentan con impedimento de carácter personal⁴⁶ de conformidad con el numeral 1 del numeral 30.1 del artículo 30 de la Ley N° 32069, Ley General de Contrataciones Públicas, de acuerdo a lo siguiente:**

[NOMBRE DEL PARIENTE 1] con DNI [...] con CARGO [...] en la ENTIDAD [...] que a la fecha de la presente declaración cuenta con impedimento de carácter personal del Tipo **[CONSIGNAR 1A, 1B, 1C, 1D, 1E, 1F, y 1G, según corresponda]** de conformidad con el inciso 1 del numeral 30.1 del artículo 30 de la Ley N° 32069 Ley General de Contrataciones Públicas.

[NOMBRE DEL PARIENTE 2] con DNI [...] con CARGO [...] en la ENTIDAD [...] que a la fecha de la presente declaración cuenta con impedimento de carácter personal del Tipo **[CONSIGNAR 1A, 1B, 1C, 1D, 1E, 1F, y 1G, según corresponda]** de conformidad con el inciso 1 del numeral 30.1 del artículo 30 de la Ley N° 32069 Ley General de Contrataciones Públicas.

Sin perjuicio de ello, **DECLARO BAJO JURAMENTO** lo siguiente:

Me encuentro exceptuado del impedimento por razón de parentesco, en razón [INDICAR SUPUESTO: HABER EJECUTADO UN CONTRATO DERIVADO DE UN PROCEDIMIENTO DE SELECCIÓN COMPETITIVO O NO COMPETITIVO / HABER EJECUTADO CUATRO CONTRATOS MENORES EN EL MISMO TIPO DE OBJETO AL QUE POSTULA] dentro de los dos años previos a la convocatoria del procedimiento de selección, contratación directa o a la adjudicación de un contrato menor] conforme al inciso 2 del numeral 30.1 del artículo 30 de la Ley N° 32069⁴⁷, Ley General de Contrataciones Públicas, lo cual acredito documentalmente, de conformidad con el numeral 39.4 del artículo 39 del Reglamento de la Ley N° 32069, Ley General de Contrataciones del Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

⁴⁴ Numeral 39.4 del artículo 39 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

⁴⁵ Se entiende pariente a aquellos hasta el segundo grado de consanguinidad y segundo de afinidad, lo que incluye al cónyuge, al conviviente, y al progenitor del hijo.

⁴⁶ Aplicables a autoridades, funcionarios o servidores públicos de acuerdo con lo que señala la Ley N° 32069, Ley General de Contrataciones Públicas-.

[CONSIGNAR EL DETALLE DE LOS DOCUMENTOS CORRESPONDIENTES]

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, nombres y apellidos del postor o
representante legal, según corresponda**

ANEXO N° 6

PRECIO DE LA OFERTA

Señores

EVALUADORES

CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC 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
TOTAL	

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

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, nombres y apellidos del postor o representante legal o común, según corresponda

Advertencia

- *En caso de que el postor reduzca su oferta, según lo previsto en el artículo 132 del Reglamento, debe presentar nuevamente este Anexo.*
- *El postor que goce de alguna exoneración legal debe indicar que su oferta no incluye el impuesto materia de la exoneración, debiendo incluir el siguiente texto:
“Mi oferta no incluye [CONSIGNAR EL IMPUESTO MATERIA DE LA EXONERACIÓN]”.*
- *En caso de procedimientos según relación de ítems, el postor puede presentar el precio de su oferta en un solo documento o documentos independientes, en los ítems que se presente.*
- *En caso de contrataciones que conllevan la ejecución de prestaciones accesorias, el postor debe detallar en el precio de su oferta, el monto correspondiente a la prestación principal y las prestaciones accesorias.*
- *En caso de divergencia entre el precio de la oferta en dígitos y en letras, prevalece este último.*

ANEXO N° 7
AUTORIZACIÓN DE RETENCIÓN COMO GARANTÍA DE FIEL CUMPLIMIENTO DEL
CONTRATO Y/O FIEL CUMPLIMIENTO DE PRESTACIONES ACCESORIAS – PROVEEDORES
MYPES

(DOCUMENTO A PRESENTAR PARA EL PERFECCIONAMIENTO DEL CONTRATO)

Señores

EVALUADORES

CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC 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, del número total de pagos a realizarse, se me aplique la retención de forma prorrateada en cada pago, con cargo a ser devuelto al finalizar el contrato, como mecanismo de garantía de fiel cumplimiento de **[PRECISAR SI ES FIEL CUMPLIMIENTO DEL CONTRATO Y/O FIEL CUMPLIMIENTO DE PRESTACIONES ACCESORIAS]**, en el marco del numeral 61.8 del artículo 61 de la Ley N° 32069, Ley General de Contrataciones Públicas, y el artículo 114 de su Reglamento, así como el artículo 3 de la Ley N° 32077, Ley que establece un medio alternativo de garantías de cumplimiento en los procesos de contratación pública de las MYPE.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, nombres y apellidos del postor o
representante legal o común, según
corresponda

Advertencia

La retención como mecanismo de garantía de fiel cumplimiento es aplicable, de acuerdo con los numerales 61.8 y 61.9 del artículo 61 de la Ley N° 32069, Ley General de Contrataciones Públicas y el artículo 114 del Reglamento, así como el artículo 3 de la Ley N° 32077, Ley que establece un medio alternativo de garantías de cumplimiento en los procesos de contratación pública de las MYPE, siempre que:

- *El plazo de la prestación sea igual o mayor de sesenta días calendario.*
- *Se consideren, según corresponda, al menos dos pagos a favor del contratista o dos valorizaciones periódicas en función del avance de obra.*
- *Cuando se adjudique la buena pro a un proveedor que califique como micro o pequeña empresa, procede la retención con independencia del monto de la contratación.*

ANEXO N° 8

DECLARACIÓN JURADA DE PRESENTACIÓN DE FIDEICOMISO COMO GARANTÍA DE FIEL CUMPLIMIENTO DEL CONTRATO

(DOCUMENTO A PRESENTAR PARA EL PERFECCIONAMIENTO DEL CONTRATO)

Señores

EVALUADORES

CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC 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]**, declaro bajo juramento el compromiso de presentar la constitución de un fideicomiso como mecanismo de garantía de fiel cumplimiento del contrato, en un plazo no mayor a veinte días hábiles contabilizados desde el día siguiente de perfeccionado el mismo, en el marco de los artículos 116 y 138 del Reglamento de la Ley N° 32069 Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

[CONSIGNAR CIUDAD Y FECHA]

.....
**Firma, nombres y apellidos del postor o
representante legal o común, según
corresponda**

Advertencia

El fideicomiso es aplicable, de acuerdo con los artículos 116 y 138 del Reglamento de la Ley N° 32069, siempre que el plazo de la ejecución contractual sea mayor a noventa días calendario.

ANEXO N° 9

AUTORIZACIÓN DE NOTIFICACIONES DURANTE LA EJECUCIÓN CONTRACTUAL MEDIANTE CORREO ELECTRÓNICO

(DOCUMENTO A PRESENTAR PARA EL PERFECCIONAMIENTO DEL CONTRATO)

Señores

EVALUADORES

CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC 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]**

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, nombres y apellidos del postor o
representante legal o común, según
corresponda

ANEXO N° 10

ELECCIÓN DE INSTITUCIÓN ARBITRAL⁴⁸

(DOCUMENTO A PRESENTAR PARA EL PERFECCIONAMIENTO DEL CONTRATO)

Señores

EVALUADORES

CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC 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], elijo la institución arbitral del listado proporcionado por la entidad contratante:

[INDICAR LA RAZON SOCIAL DE LA INSTITUCIÓN ARBITRAL ELEGIDA, DE ACUERDO AL LISTADO DEL NUMERAL 3.3 DEL CAPÍTULO III DE LA SECCIÓN ESPECÍFICA DE LAS BASES]

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, nombres y apellidos del postor o
representante legal o común, según corresponda

⁴⁸ Para la elección de la institución arbitral, la entidad contratante debe tomar en cuenta, como aspectos relevantes, lo previsto en el literal d) del artículo 77 (Requisitos para resolver controversias en contrataciones públicas) y el numeral 84.1 del artículo 84 (Reglas aplicables al arbitraje) de la Ley.

ANEXO N° 11

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Señores

EVALUADORES

CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC S.A.-PRIMERA CONVOCATORIA

Presente.-

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

N°	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ⁴⁹	FECHA DE LA CONFORMIDAD DE SER EL CASO ⁵⁰	EXPERIENCIA PROVENIENTE DE:	MONEDA	IMPORTE ⁵¹	TIPO DE CAMBIO VENTA ⁵²	MONTO FACTURADO ACUMULADO ⁵³
1										
2										
3										
4										
5										
6										
7										
8										

⁴⁹ Se refiere a la fecha de suscripción del contrato, de la emisión de la Orden de Servicio o de cancelación del comprobante de pago, según corresponda.

⁵⁰ **Únicamente**, cuando la fecha del perfeccionamiento del contrato sea previa a los quince 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.

⁵¹ Se refiere al monto del contrato ejecutado incluido adicionales y reducciones, de ser el caso.

⁵² 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 Servicio o de cancelación del comprobante de pago, según corresponda.

⁵³ Consignar en la moneda establecida en las bases.

Nº	CLIENTE	OBJETO DEL CONTRATO	N° CONTRATO / O/S / COMPROBANTE DE PAGO	FECHA DEL CONTRATO O CP ⁴⁹	FECHA DE LA CONFORMIDAD DE SER EL CASO ⁵⁰	EXPERIENCIA PROVENIENTE DE:	MONEDA	IMPORTE ⁵¹	TIPO DE CAMBIO VENTA ⁵²	MONTO FACTURADO ACUMULADO ⁵³
9										
10										
...										
20										
TOTAL										

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, nombres y apellidos del postor o representante legal o común, según corresponda

Advertencia

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de que el postor sea sucursal considerando que ambas constituyen la misma persona jurídica conforme a lo previsto en el artículo 396 de la Ley N° 26887, Ley General de Sociedades, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente. Del mismo modo, en aplicación de lo previsto en la mencionada Ley, 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.

ANEXO N° 14

DECLARACIÓN JURADA

Señores

EVALUADORES

CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC 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 72.3 del artículo 72 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF.

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, nombres y apellidos del postor o representante legal, según corresponda

Advertencia

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 Públicas con sanción vigente en <http://portal.osce.gob.pe/rnp/content/relación-de-proveedores-sancionados>. También le asiste dicha facultad a la dependencia encargada de las contrataciones o al órgano de la entidad contratante al que se le haya asignado la función de verificación de la oferta presentada por el postor ganador de la buena pro.

ANEXO N° 15
DECLARACIÓN JURADA DE ACTUALIZACIÓN DE DESAFECTACIÓN DE
IMPEDIMENTO

(DOCUMENTO A PRESENTAR PARA EL PERFECCIONAMIENTO DEL CONTRATO)

Señores

DEPENDENCIA ENCARGADA DE LAS CONTRATACIONES

CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC S.A.-PRIMERA CONVOCATORIA

Presente.-

El que suscribe, [...], postor y/o representante legal de **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]**, identificado con **[CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD]**, con poder inscrito en la sede registral de **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]** en la Ficha N° **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]** Asiento N° **[CONSIGNAR EN CASO DE SER PERSONA JURÍDICA]**, **declaro que tengo los siguientes parientes⁵⁴, los cuales cuentan con impedimento de carácter personal⁵⁵ de conformidad con el numeral 1 del numeral 30.1 del artículo 30 de la Ley N° 32069, Ley General de Contrataciones Públicas, de acuerdo a lo siguiente:**

[NOMBRE DEL PARIENTE 1] con DNI [...] con CARGO [...] en la ENTIDAD [...] que a la fecha de la presente declaración es un impedido de carácter personal del Tipo **[CONSIGNAR 1A, 1B, 1C, 1D, 1E, 1F, y 1G, SEGÚN CORRESPONDA]** .

[NOMBRE DEL PARIENTE 2] con DNI [...] con CARGO [...] en la ENTIDAD [...] que a la fecha de la presente declaración es un impedido de carácter personal del Tipo **[CONSIGNAR 1A, 1B, 1C, 1D, 1E, 1F, y 1G, SEGÚN CORRESPONDA]** ..

Sin perjuicio de ello, **DECLARO BAJO JURAMENTO** lo siguiente:

A la fecha me encuentro exceptuado del impedimento por razón de parentesco, en razón de **[INDICAR SUPUESTO: HABER EJECUTADO UN CONTRATO DERIVADO DE UN PROCEDIMIENTO DE SELECCIÓN COMPETITIVO O NO COMPETITIVO / HABER EJECUTADO CUATRO CONTRATOS MENORES EN EL MISMO TIPO DE OBJETO AL QUE POSTULA]** dentro de los dos años previos a la convocatoria del procedimiento de selección, contratación directa o a la adjudicación de un contrato menor] conforme al inciso 2 del numeral 30.1 del artículo 30 de la Ley N° 32069⁵⁶, Ley General de Contrataciones Públicas, lo cual acredito documentalmente, de conformidad con el numeral 39.4 del artículo 39 del Reglamento de la Ley N° 32069, Ley General de Contrataciones del Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

En ese sentido, mediante el presente cumplo con presentar la acreditación documental correspondiente:

[CONSIGNAR EL DETALLE DE LOS DOCUMENTOS CORRESPONDIENTES]

[CONSIGNAR CIUDAD Y FECHA]

⁵⁴ Se entiende pariente a aquellos hasta el segundo grado de consanguinidad y segundo de afinidad, lo que incluye al cónyuge, al conviviente, y al progenitor del hijo.

⁵⁵ Aplicables a autoridades, funcionarios o servidores públicos de acuerdo con lo que señala la Ley N° 32069-.

⁵⁶ Conforme el numeral 2 "Impedimentos en razón del parentesco" del numeral 30.1 del artículo 30 de la Ley N° 32069, Ley General de Contrataciones Públicas.

.....
**Firma, nombres y apellidos del postor o
representante legal, según corresponda**

ANEXO N° 18⁵⁷

DECLARACIÓN JURADA SOBRE INAPLICACIÓN DEL IMPEDIMENTO TIPO 4.D DEL INCISO 4 DEL NUMERAL 30.1 DEL ARTÍCULO 30 DE LA LEY N° 32069 REFERIDO A LA INSCRIPCIÓN EN EL REGISTRO DE DEUDORES ALIMENTARIOS MOROSOS – REDAM

(Documento a presentar para el perfeccionamiento del contrato en caso de proveedores con procesos de alimentos en ejecución de sentencia)

Señores

EVALUADORES

CONCURSO PÚBLICO DE SERVICIOS N°007.2025.CORPAC S.A.-PRIMERA CONVOCATORIA

Presente.-

El que suscribe, [...], postor y/o apoderado de **[CONSIGNAR EL NOMBRE DE LA PERSONA NATURAL QUE OTORGA EL PODER, DE SER EL CASO]**, identificado con **[CONSIGNAR TIPO DE DOCUMENTO DE IDENTIDAD] N° [CONSIGNAR NÚMERO DE DOCUMENTO DE IDENTIDAD]**, con poder inscrito en la localidad de **[CONSIGNAR EN CASO DE CONTAR CON APODERADO]** en la Ficha N° **[CONSIGNAR EN CASO DE CONTAR CON APODERADO]** Asiento N° **[CONSIGNAR EN CASO DE CONTAR CON APODERADO]**, **DECLARO BAJO JURAMENTO** que no me resulta aplicable el impedimento Tipo 4.D del inciso 4 del numeral 30.1 del artículo 30 de la Ley, referido a las personas inscritas en el Registro de Deudores Alimentarios Morosos del Poder Judicial (Redam), considerando lo siguiente:

[EL PROVEEDOR DEBE CONSIGNAR LA INFORMACIÓN SÓLO UNA DE LAS OPCIONES QUE SE ESTABLECEN A CONTINUACIÓN, SEGÚN SEA EL CASO]:

- Que, se ha remitido el/la **[CONSIGNAR LA DENOMINACIÓN EXACTA DEL DOCUMENTO REMITIDO POR EL PROVEEDOR AL JUZGADO A CARGO DEL PROCESO DE ALIMENTOS]** con fecha de recepción **[CONSIGNAR FECHA DE RECEPCIÓN]** dirigido/a al **[CONSIGNAR LOS DATOS DE IDENTIFICACIÓN DEL JUZGADO A CARGO DEL PROCESO DE ALIMENTOS QUE CORRESPONDA]**, mediante el cual se informó la cancelación de la deuda alimentaria derivada del proceso de alimentos seguido por **[CONSIGNAR LOS DATOS DE LA PARTE DEMANDANTE DEL PROCESO DE ALIMENTOS]**, para lo cual me sujeto al principio de presunción de veracidad. Se adjunta el cargo de recepción del indicado documento.
- Que, sí me encuentro en el registro de deudores alimentario moroso, por lo que; autorizo se me descuenta del pago que me corresponde como contraprestación del contrato derivado del presente procedimiento de selección, el monto de la pensión mensual fijada en el proceso de alimentos seguido por **[CONSIGNAR LOS DATOS DE LA PARTE DEMANDANTE DEL PROCESO DE ALIMENTOS]** ante el **[CONSIGNAR LOS DATOS DE IDENTIFICACIÓN DEL JUZGADO CORRESPONDIENTE]**, para lo cual adjunto:
 - a) La sentencia emitida por el **[CONSIGNAR LOS DATOS DE IDENTIFICACIÓN DEL JUZGADO A CARGO DEL PROCESO DE ALIMENTOS QUE CORRESPONDA]** en

⁵⁷ De conformidad con lo previsto en el numeral 39.2 del artículo 39 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas.

el trámite del proceso de alimentos seguido en el expediente **[CONSIGNAR EL NÚMERO DE EXPEDIENTE JUDICIAL]**

- b) La información complementaria solicitada por la entidad contratante para realizar el descuento, la que comprende lo siguiente: **[LA ENTIDAD CONTRATANTE DEBE CONSIGNAR LA INFORMACIÓN QUE REQUIERA DEL PROVEEDOR PARA HACER EFECTIVO EL DESCUENTO]**

[CONSIGNAR CIUDAD Y FECHA]

.....
Firma, nombres y apellidos del postor o
apoderado, según corresponda