

PLIEGO DE BASES Y CONDICIONES

Convocante:

**Servicio Nacional de Promocion Profesional (SNPP) / Ministerio
de Trabajo, Empleo y Seguridad Social
Servicio Nacional de Promocion Profesional**

Nombre de la Licitación:

**ADQUISICIÓN DE SISTEMA DE GESTIÓN DE
SEGURIDAD DE LA INFORMACIÓN (SGSI) Y UN
CENTRO DE OPERACIONES DE SEGURIDAD (SOC)
PARA EL SNPP - PLURIANUAL
(versión 1)**

ID de Licitación:

473102



Modalidad:

Licitación Pública Nacional

Publicado el:

25/09/2025

*"Pliego para la Adquisición de Bienes y/o Servicios - CONVENCIONAL - Ley N°
7021/22."
Versión 3*

RESUMEN DEL LLAMADO

Datos de la Convocatoria

ID de Licitación:	473102	Nombre de la Licitación:	ADQUISICIÓN DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) Y UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) PARA EL SNPP - PLURIANUAL
Convocante:	Servicio Nacional de Promocion Profesional (SNPP) / Ministerio de Trabajo, Empleo y Seguridad Social	Categoría:	43000000 - Tecnologías de Informacion, Telecomunicaciones y Radiodifusiones
Unidad de Contratación:	Servicio Nacional de Promocion Profesional	Tipo de Procedimiento:	LPN - Licitación Pública Nacional

Etapas y Plazos

Lugar para Realizar Consultas:	CONSULTAS VIRTUALES A TRAVÉS DEL PORTAL	Fecha Límite de Consultas:	09/10/2025 12:00
Lugar de Entrega de Ofertas:	MOLAS LÓPEZ N° 480 ESQ. TTE CIRILO GILL - EDIFICIO DEL SNPP - OFICINA DE LA UOC - PRIMER BLOQUE.	Fecha de Entrega de Ofertas:	15/10/2025 08:00
Lugar de Apertura de Ofertas:	MOLAS LÓPEZ N° 480 ESQ. TTE CIRILO GILL - EDIFICIO DEL SNPP - OFICINA DE LA UOC - PRIMER BLOQUE.	Fecha de Apertura de Ofertas:	15/10/2025 08:15

Adjudicación y Contrato

Sistema de Adjudicación:	Total	Anticipo:	No se otorgará anticipo
Vigencia del Contrato:	Hasta cumplimiento total de obligaciones		

Datos del Contacto

Nombre:	MÓNICA BEATRIZ OSORIO CARDOZO	Cargo:	DIRECTORA INTERINA - DIRECCIÓN DE LA UOC
Teléfono:	0981 813618	Correo Electrónico:	uocsnp2@gmail.com

DATOS DE LA CONVOCATORIA

Los Datos de la Licitación constituye la información proporcionada por la convocante para establecer las condiciones a considerar del proceso particular, y que sirvan de base para la elaboración de las ofertas por parte de los potenciales oferentes.

Datos de la Convocatoria

Los datos de la licitación serán consignados en esta sección y en el Sistema de Información de Contrataciones Públicas (SICP), los mismos forman parte de los documentos del presente procedimiento de contratación.

Difusión de los documentos de la Convocatoria

Todos los datos y documentos de este procedimiento de contratación deben ser obtenidos directamente del (SICP). Es responsabilidad del oferente examinar todos los documentos y la información de la convocatoria que obren en el mismo.

Contratación Pública Sostenibles - CPS

Las compras públicas juegan un papel fundamental en el desarrollo sostenible, así como en la promoción de estilos de vida sostenibles.

El Estado, por medio de las actividades de compra de bienes y servicios sostenibles, busca incentivar la generación de nuevos emprendimientos, modelos de negocios innovadores y el consumo sostenible. La introducción de criterios y especificaciones técnicas con consideraciones sociales, ambientales y económicas tiene como fin contribuir con el Desarrollo Sostenible en sus tres dimensiones.

El símbolo "CPS" en este pliego de bases y condiciones, es utilizado para indicar criterios o especificaciones sostenibles.

Criterios sociales y económicos:

- Los oferentes deberán garantizar la no contratación de menores, de conformidad a lo establecido en las normativas legales vigentes, conforme a lo indicado en el formulario de oferta.
- Los oferentes deberán cumplir con las disposiciones legales vigentes, garantizando a sus trabajadores condiciones de trabajo dignas y justas. Esto incluye el pago de salarios adecuados, el cumplimiento de cargas sociales, la provisión de uniformes y equipos de protección individual, la bonificación familiar cuando corresponda, el respeto a la jornada laboral y la aplicación de condiciones especiales para quienes desempeñan trabajos insalubres o peligrosos, así como la remuneración correspondiente por jornada nocturna, conforme a lo indicado en el formulario de oferta.
- Los oferentes adjudicados deberán adoptar medidas para la creación de empleo local y el uso de suministros locales, siempre y cuando exista viabilidad técnica y económica.

Criterios ambientales:

- El oferente adjudicado deberá cumplir con los lineamientos ambientales, incluidos en el ordenamiento jurídico o dictado por la institución.

- El oferente adjudicado deberá asegurar que todos los residuos generados por sus actividades sean adecuadamente gestionados (identificados, segregados y destinados) y buscar su minimización en la fuente, por medio de prácticas como la modificación de los procesos de producción, manutención y de las instalaciones utilizadas, además de la sustitución, conservación, reciclaje o reutilización de materiales.

Conducta empresarial responsable:

Los oferentes deberán observar los más altos niveles de integridad, así como altos estándares de conducta de negocios, ya sea durante el procedimiento de licitación o la ejecución de un contrato. En tal sentido, se comprometen a:

- Abstenerse de ofrecer, prometer, entregar o solicitar, de manera directa o indirecta, pagos ilícitos, a funcionarios públicos, con el fin de obtener o mantener un contrato, en todos los casos sea o no una ventaja ilegítima o indebida.
- Abstenerse de solicitar, recibir o aceptar ventajas indebidas de funcionarios públicos o de empleados de sus socios comerciales.
- Promover o fomentar políticas, programas o códigos de conducta orientados a la prevención de la corrupción, promoción de la integridad y fomento de la transparencia dentro de todas sus actividades, sean comerciales o no. Asimismo, podrá promover mecanismos de monitoreo y evaluación de cumplimiento de los mismos.
- Asegurar que todos los recursos destinados a la ejecución de un contrato público provengan de fuentes lícitas.
- Promover estándares de conducta responsable en sus propios proveedores, creando una cadena de suministro ética y sostenible.
- Garantizar que los fondos derivados de una licitación no serán utilizados para fines ilícitos.

Aclaración de los documentos de la convocatoria

1. Consultas electrónicas

Todo potencial oferente que necesite alguna aclaración sobre la convocatoria o el pliego de bases y condiciones podrá solicitarla a la convocante a través del Sistema de Información de las Contrataciones Públicas (SICP) desde el día de la publicación de la convocatoria o de sus adendas, y hasta el plazo establecido por la convocante. Las consultas recibidas deberán ser respondidas y publicadas directamente a través del SICP.

2. Respuestas y aclaraciones

Las aclaraciones realizadas durante los procedimientos de contratación no serán consideradas modificaciones a las bases de la contratación. Sin embargo, a los efectos legales, la aclaración será considerada parte integrante del documento cuyo contenido aclare.

3. Adendas y prórrogas del tope para consultas.

Cuando la Convocante modifique especificaciones técnicas, criterios de evaluación u otros aspectos sustanciales del pliego de bases y condiciones, deberá prorrogar de manera obligatoria el tope para la realización de consultas, a fin de garantizar los plazos de difusión mínimos establecidos en la reglamentación de la DNCP.

4. Emisión de aclaraciones sobre Adendas

Cuando se prorrogue el plazo tope de consultas debido a una adenda modificatoria de las bases y condiciones, la convocante deberá analizar únicamente las consultas que se refieran al contenido de la adenda. En caso de recibir consultas relacionadas con lo establecido en las bases originalmente, la convocante no estará obligada a analizarlas, debiendo el oferente remitirse a las bases originales.

5. Junta de aclaraciones

La convocante podrá establecer una Junta de Aclaraciones para la evacuación de consultas sobre la convocatoria y los pliegos de bases y condiciones, de forma adicional a las consultas realizadas, debiendo fijar la fecha, hora y lugar de realización en el SICP.

La convocante podrá optar por responder las consultas en la Junta de Aclaraciones o diferirlas para responderlas conforme a los plazos de respuesta o emisión de adendas. En todos los casos, se deberá levantar un acta circunstanciada.

La inasistencia a la Junta de Aclaraciones no será motivo de descalificación de la oferta.

Formato y firma de la oferta

1. El formulario de oferta y la lista de precios serán firmados, física o electrónicamente, según corresponda por el oferente o por las personas debidamente facultadas para firmar en nombre del oferente.
2. No serán descalificadas las ofertas que no hayan sido firmadas en documentos considerados no sustanciales.
3. Los textos entre líneas, tachaduras o palabras superpuestas serán válidos solamente si llevan la firma de la persona que firma la oferta.
4. La falta de foliatura no podrá ser considerada como motivo de descalificación de las ofertas.
5. Cuando la Garantía de Mantenimiento de Ofertas sea instrumentada a través de Declaración Jurada, deberá estar firmada en todas sus páginas.

Plazo para presentar las ofertas

Las ofertas deberán ser presentadas en la fecha y hora que se indican en el SICP.

La convocante podrá, extender el plazo originalmente establecido para la presentación de ofertas mediante la prórroga de fecha tope o la postergación de la apertura de ofertas.

En este caso todos los derechos y obligaciones de la convocante y de los oferentes previamente sujetos a la fecha límite original para presentar las ofertas, quedarán sujetos a la nueva fecha prevista.

Cuando la presentación de oferta sea electrónica la misma deberá sujetarse a la reglamentación vigente.

Oferentes en consorcio

Dos o más interesados podrán unirse temporalmente para presentar una oferta sin crear una persona jurídica distinta y deberán designar a uno de sus integrantes como líder quien suscribirá la oferta y los documentos relativos al procedimiento de contratación. La inscripción en el Registro de Proveedores del Estado por parte de todos los miembros del consorcio, constituye requisito previo para la presentación de las ofertas, los cuales deberán encontrarse activos en el Registro. Se deberá realizar el procedimiento de activación del consorcio directamente a través del Registro de Proveedores.

Para ello deberán presentar una escritura pública de constitución que reúna las características previstas en el Decreto reglamentario o un acuerdo de intención de participación en contrato de consorcio, el cual se deberá formalizar por escritura pública en caso de resultar adjudicados, antes de la firma del contrato.

Los integrantes de un consorcio no podrán presentar ofertas individuales ni conformar más de un consorcio para un mismo lote o ítem, lo que no impide que puedan presentarse en diferentes partidas de manera individual o como miembro de otro consorcio.

En todo lo demás deberán ajustarse a lo dispuesto en la normativa legal vigente.

Idioma de la oferta

La oferta deberá ser presentada en idioma castellano.

La convocante permitirá con la oferta, la presentación de catálogos, anexos técnicos o folletos en idioma distinto al castellano y su traducción:

No Aplica

Lista de Precios

1. Para la cotización el oferente deberá ajustarse a los requerimientos que se indican a continuación:

- a) El precio cotizado deberá ser el mejor precio posible, considerando que en la oferta no se aceptará la inclusión de descuentos de ningún tipo.
- b) En el caso del sistema de adjudicación por la totalidad de los bienes y/o servicios requeridos, el oferente deberá cotizar en la lista de precios todos los ítems, con sus precios unitarios y totales correspondientes.
- c) En el caso del sistema de adjudicación por lotes, el oferente cotizará en la lista de precios uno o más lotes, e indicará todos los ítems del lote ofertado con sus precios unitarios y totales correspondientes. En caso de no cotizar uno o más lotes, los lotes no cotizados no requieren ser incorporados al listado de ítems.
- d) En el caso del sistema de adjudicación por ítems, el oferente podrá ofertar por uno o más ítems, en cuyo caso deberá cotizar el precio unitario y total de cada uno o más ítems, los ítems no cotizados no requieren ser incorporados al listado de ítems.
- e) En todos los casos, independiente al sistema de adjudicación, el oferente deberá indicar el CPEN respectivo al ítem ofertado, en caso de contar. Dicho atributo tendrá carácter formal siendo susceptible de aclaraciones por parte del comité de evaluación.

2. Los precios indicados en la lista de precios serán consignados separadamente, de acuerdo a lo previsto en el SICP y según se detalla a continuación:

- a) El precio de bienes y/o servicios cotizados, incluidos todos los derechos de aduana, los impuestos al valor agregado o de otro tipo pagados o por pagar sobre los componentes y materia prima utilizada en la fabricación o ensamblaje de los bienes;
- b) Todo impuesto al valor agregado u otro tipo de impuesto que obligue la República del Paraguay a pagar sobre los bienes en caso de ser adjudicado el contrato; además, se deberá indicar los ítems exentos de IVA, cuando los hubiere y;
- c) El precio de otros servicios conexos (incluyendo su impuesto al valor agregado), si los hubiere, enumerados en los datos de la licitación.

3. En caso de indicarse en el SICP, que se utilizará el atributo de contrato abierto, cuando se realice por montos mínimos y máximos deberán indicarse el precio unitario de los bienes y/o servicios ofertados; y en caso de realizarse por cantidades mínimas y máximas, deberán cotizarse los precios unitarios y los totales se calcularán multiplicado los precios unitarios por la cantidad máxima correspondiente.

4. El precio del contrato que perciba el proveedor por los bienes y/o servicios suministrados en virtud del contrato no podrá ser diferente a los precios unitarios cotizados en su oferta, excepto por cualquier ajuste previsto en el mismo.

5. En caso que se requiera el desglose de los componentes de los precios será con el propósito de facilitar a la convocante la comparación de las ofertas.

6. En las contrataciones internacionales los oferentes no domiciliados en el territorio de la República deberán manifestar en su oferta que los precios que presentan en su propuesta económica no se cotizan en condiciones de prácticas desleales

de comercio internacional en su modalidad de discriminación de precios o subsidios.

Abastecimiento simultáneo

En caso de que se opte por el sistema de abastecimiento simultáneo, en éste apartado se deberá indicar la manera de distribución de los mismos:

No Aplica

Moneda de la oferta y pago

La moneda de la oferta y pago será:

En guaraníes para todos los oferentes.

La cotización en moneda diferente de la indicada en este apartado será causal de rechazo de la oferta. Si la oferta seleccionada es en guaraníes, la oferta se deberá expresar en números enteros, no se aceptarán cotizaciones en decimos y céntimos.

Copias de la oferta - CPS

El oferente presentará su oferta original. Adicionalmente, la convocante podrá requerir copias de las ofertas en la cantidad indicada en este apartado, las copias deberán estar indicadas como tales.

Cuando la presentación de las ofertas se realice a través del módulo de Oferta Electrónica, la convocante no requerirá de copias.

Cantidad de copias requeridas:

No Aplica

Método de presentación de ofertas

El método de presentación de ofertas para esta convocatoria será:

Un sobre

En caso de presentación física, los sobres deberán:

1. Indicar el nombre, RUC y la dirección del oferente;
2. Estar dirigidos a la convocante;
3. Llevar la identificación específica del proceso de contratación indicado en el SICP; y
4. Llevar una advertencia de no abrir antes de la hora y fecha de apertura de ofertas.
5. Identificar si se trata de un sobre técnico o económico.

Para los casos de consorcios con acuerdo de intención, los sobres deberán contemplar el RUC provisorio generado en el Registro de Proveedores.

La convocante podrá determinar el método de presentación de ofertas en un sobre o en doble sobre. En este último caso, el primer sobre contendrá la oferta técnica, incluyendo los documentos que acrediten la personería del oferente y el segundo sobre, contendrá la oferta económica. En caso de presentación de ofertas físicas, las mismas deberán ser entregadas a la convocante en sobres cerrados. Cuando las mismas deban ser presentadas en doble sobre, la convocante deberá resguardar las ofertas técnicas y económicas hasta su apertura.

En caso de la utilización del módulo de ofertas electrónicas, la misma se registrará por las disposiciones establecidas en la normativa vigente y la guía de ofertas electrónicas.

Si los sobres no están cerrados e identificados como se requiere, la convocante deberá dejar constancia de ello en el acto de apertura y no se responsabilizará en caso de que la oferta se extravíe o sea abierta prematuramente, sin embargo, cuando el sobre no cuente con el RUC, se podrá subsanar dicha omisión al momento de la presentación.

Documentos de la oferta

El pliego, sus adendas y aclaraciones no forman parte de la oferta, por lo que no se exigirá la presentación de copias de los mismos con la oferta.

1. Constancia del Perfil del proveedor.

1.1 Ofertas físicas

Los oferentes inscriptos en el Registro de Proveedores del Estado, podrán presentar con su oferta, la Constancia del Perfil del Proveedor que contiene el reporte de los documentos obrantes en el Registro. Con su presentación en la oferta, dicha constancia reemplazará a los documentos solicitados por la convocante en el presente pliego.

Será considerada válida la Constancia que se presente con firma manuscrita o electrónica cualificada por él o los representantes legales.

1.2 Ofertas electrónicas

Cuando la presentación de oferta sea electrónica, no será necesaria la presentación física de la Constancia y el oferente deberá sujetarse a la reglamentación vigente en la materia.

2. Confidencialidad de documentos.

Los oferentes deberán indicar en su oferta, qué documentos que forman parte de la misma son de carácter reservado e invocar la norma que ampara dicha reserva, para así dar cumplimiento a lo estipulado en la Ley N° 5282/14 "DE LIBRE ACCESO CIUDADANO A LA INFORMACIÓN PÚBLICA Y TRANSPARENCIA GUBERNAMENTAL". Si el oferente no hace pronunciamiento expreso amparado en la Ley, se entenderá que toda su oferta y documentación es pública.

Ofertas Alternativas

Se permitirá la presentación de oferta alternativa, según los siguientes criterios a ser considerados para la evaluación de la misma:

No Aplica

Periodo de validez de las ofertas

Las ofertas deberán mantenerse válidas por:

90

días corridos.

Las ofertas se deberán mantener válidas por el periodo indicado en el presente apartado, a partir de la fecha límite para la presentación de ofertas, establecido por la convocante. Toda oferta con un periodo menor será rechazada.

La convocante en circunstancias excepcionales podrá solicitar, por escrito, al oferente que extienda el periodo de validez de la oferta, por lo tanto la Garantía de Mantenimiento de la Oferta deberá ser también prorrogada.

El oferente puede rehusarse a tal solicitud sin que se le haga efectiva su Garantía de Mantenimiento de Oferta. A los oferentes que acepten la solicitud de prórroga no se les solicitará ni permitirá que modifiquen sus ofertas.

Garantías: instrumentación, plazos y ejecución.

1. Instrumentación y porcentaje

1.1 La Garantía de Mantenimiento de Oferta deberá expedirse por el equivalente 5% (cinco por ciento) del monto total de la oferta. El oferente debe adoptar cualquiera de las siguientes formas:

- a. Garantía bancaria emitida por un banco establecido en la República del Paraguay, la que deberá ajustarse a las condiciones establecidas por la DNCP.
- b. Póliza de seguros emitida por una compañía autorizada a operar y emitir pólizas de seguros de caución en la República del Paraguay. La póliza deberá ajustarse a las condiciones establecidas por la DNCP.
- c. En los procedimientos, cuyo monto de estimación de la contratación sea inferior a los dos mil (2.000) jornales mínimos, se admitirá la instrumentación de las garantías de mantenimiento de ofertas a través de Declaraciones Juradas con certificación de firma por Escribano Público. La certificación de firma podrá corresponder a la misma fecha del documento certificado o a una fecha posterior.
- d. En caso de utilizarse el Módulo de Ofertas Electrónicas, las declaraciones juradas serán generadas y firmadas a través del módulo y no requerirán certificación de firmas.

1.2 En los casos de contratos abiertos las garantías se registrarán por lo dispuesto en el Decreto Reglamentario y la reglamentación emitida por la DNCP para el efecto.

1.3 En caso de instrumentarse las garantías a través de Garantía Bancaria o Declaración Jurada, deberá estar sustancialmente de acuerdo con el formulario incluido en la Sección "Formularios".

2. Garantía de mantenimiento de ofertas en consorcios

2.1. En caso de consorcios, la garantía de mantenimiento de ofertas deberá ser presentada de la siguiente manera:

- a. Consorcio constituido por escritura pública: deberán emitir a nombre del consorcio legalmente constituido por escritura pública o del gestor y representante del consorcio (Empresa líder), designado en la escritura pública.
- b. Consorcio con acuerdo de intención de participación en contrato de consorcio: deberán emitir a nombre del gestor

y representante del consorcio (empresa líder), designado en el acuerdo.

3. Ejecución de la Garantía de mantenimiento de ofertas

3.1. La Garantía de Mantenimiento de Ofertas podrá ser ejecutada:

- a. Si el oferente altera las condiciones de su oferta,
- b. Si el oferente retira su oferta durante el período de validez de ofertas,
- c. Si no acepta la corrección aritmética del precio de su oferta, en caso de existir, o
- d. Si el adjudicatario no procede, por causa imputable al mismo a:

d.1 Firmar el contrato,

d.2 Suministrar los documentos indicados en las bases de la contratación para la firma del contrato,

d.3 Suministrar en tiempo y forma la garantía de cumplimiento de contrato,

d.4 Cuando se comprobare que las declaraciones juradas presentadas por el oferente adjudicado con su oferta sean falsas,

d.5 No se formaliza el consorcio por escritura pública antes de la firma del contrato.

4. Las Garantías tanto de Mantenimiento de Oferta, Cumplimiento de Contrato o de Anticipo, sea cual fuere la forma de instrumentación adoptada, deberá ser pagadera ante solicitud escrita de la convocante donde se haga constar el monto reclamado, cuando se tenga acreditada una de las causales de ejecución de la garantía. En estos casos será requisito que previamente el oferente sea notificado del incumplimiento y la intimación de que se hará efectiva la ejecución del monto asegurado.

Periodo de Validez de la Garantía de Mantenimiento de Oferta

El plazo de validez de la Garantía de Mantenimiento de Oferta será de:

120

días corridos.

El oferente deberá presentar como parte de su oferta una Garantía de Mantenimiento de acuerdo al porcentaje indicado para ello en el SICP y por el plazo indicado en este apartado.

El plazo mínimo de validez será de al menos 30 días posteriores al plazo de validez establecido para las ofertas.

Subcontratación

El porcentaje permitido para la subcontratación será de:

No Aplica

El oferente podrá indicar junto con la oferta las personas a ser subcontratadas, o, en la etapa contractual previa a la autorización por parte de la contratante. El formulario de personas a subcontratar/subcontratadas, deberá ser presentado de acuerdo a la etapa en la que se indique la subcontratación, siendo susceptible de evaluación respecto a las inhabilidades del Art 21 de la Ley N°

Retiro, sustitución y modificación de las ofertas

1. Ofertas físicas.

1.1 Un oferente podrá retirar, sustituir o modificar su oferta después de presentada mediante el envío de una comunicación por escrito, debidamente firmada por el representante autorizado. La sustitución o modificación correspondiente de la oferta deberá acompañar dicha comunicación por escrito.

1.2. Todas las comunicaciones deberán ser:

- a) Presentadas conforme a la forma de presentación e identificación de las ofertas y además los respectivos sobres deberán estar marcados "RETIRO", "SUSTITUCION" o "MODIFICACION";
- b) Realizadas antes del plazo límite establecido para el acto de apertura de ofertas cuando las ofertas sean identificadas con "RETIRO", y;
- c) Realizadas antes del plazo límite establecido para la presentación de ofertas cuando las ofertas sean identificadas con "SUSTITUCIÓN" o "MODIFICACIÓN".

Las ofertas cuyo retiro, sustitución o modificación fuere solicitada serán devueltas sin abrir a los oferentes remitentes, durante el acto de apertura de ofertas.

1.3. Ninguna oferta podrá ser retirada durante el intervalo comprendido entre la fecha límite para el acto de apertura y la expiración del período de validez de las ofertas indicado en el Formulario de Oferta o cualquier extensión si la hubiere, caso contrario, se hará efectiva la Garantía de Mantenimiento de Oferta.

1.4. Ninguna oferta podrá ser sustituida o modificada durante el intervalo comprendido entre la fecha límite para presentar ofertas y la expiración del período de validez de las ofertas indicado en el Formulario de Oferta o cualquier extensión si la hubiere, caso contrario, se hará efectiva la Garantía de Mantenimiento de Oferta.

2. Ofertas electrónicas.

2.1. Un oferente podrá retirar, sustituir o modificar su oferta después de presentada, hasta antes de la fecha límite de presentación y apertura de ofertas, para ello deberá sujetarse a la reglamentación pertinente.

Apertura de ofertas

1. Desarrollo del acto de apertura de ofertas.

1.1. La entidad convocante procederá a la apertura de las ofertas en acto público en presencia de los oferentes o sus representantes según la hora, fecha y lugar previamente establecidos en el SICP.

1.2. Cuando la presentación de la oferta sea electrónica, el acto de apertura deberá sujetarse a la reglamentación vigente, en la hora y fecha establecida en el SICP.

1.3. Primero la convocante deberá verificar que los oferentes se encuentren inscritos en el Registro de Proveedores del Estado conforme con los datos previstos en el sobre. En caso de que un oferente no inscripto en el Registro haya presentado una oferta, la convocante deberá dejar constancia en el acta de apertura electrónica. El sobre con la oferta correspondiente no será abierto sino devuelto al oferente remitente. Esta disposición no será aplicable a los procedimientos que utilicen el módulo de ofertas electrónicas.

1.4. Luego se procederá a verificar los sobres de las ofertas recibidas, marcados como:

- a) "RETIRO": Se leerán en voz alta y el sobre con la oferta correspondiente no será abierto sino devuelto al oferente remitente. No se permitirá el retiro de ninguna oferta a menos que la comunicación de retiro contenga una autorización válida y sea leída en voz alta en el acto de apertura de las ofertas.

b) "SUSTITUCION": Se leerán en voz alta y se intercambiará con la oferta correspondiente que está siendo sustituida; la oferta sustituida no se abrirá y se devolverá al oferente remitente. No se permitirá la sustitución de ninguna oferta a menos que la comunicación de sustitución contenga una autorización válida y sea leída en voz alta en el acto de apertura de las ofertas.

c) "MODIFICACION": Se abrirán y leerán en voz alta con la oferta correspondiente. No se permitirá ninguna modificación a las ofertas a menos que la comunicación de modificación contenga una autorización válida y sea leída en voz alta en el acto de apertura de las ofertas. Solamente se considerarán en la evaluación los sobres que se abren y leen en voz alta durante el Acto de Apertura de las Ofertas.

1.5. Los representantes de los oferentes que participen en la apertura de las ofertas deberán contar con autorización suficiente para suscribir el acta y para revisar los documentos de los demás oferentes, bastando para ello la presentación de una autorización escrita del firmante de la oferta, esta autorización podrá ser incluida en el sobre oferta o ser portada por el representante.

1.6. Se solicitará a los representantes de los oferentes presentes que firmen el acta. La omisión de la firma por parte de un oferente no invalida el contenido y efecto del acta. Se distribuirá una copia del acta a todos los presentes.

1.7. Las ofertas sustituidas y modificadas, que no sean abiertas y leídas en voz alta durante el acto de apertura no podrán ser consideradas para la evaluación sin importar las circunstancias y serán devueltas sin abrir a los remitentes.

1.8. La falta de firma en un documento sustancial, es considerada una omisión sustancial que no podrá ser subsanada en ninguna oportunidad una vez abiertas las ofertas. En cuanto a la garantía de mantenimiento de oferta deberá estar debidamente extendida.

2. Comunicación del acta de apertura.

2.1. En el sistema de un solo sobre el acta de apertura deberá ser comunicada a través del SICP para su difusión, dentro de los dos (02) días hábiles de la realización del acto de apertura.

2.2. En el sistema de doble sobre, el acta de apertura técnica deberá ser comunicada a través del SICP, para su difusión, dentro de los dos (02) días hábiles de la realización del acto de apertura, se procederá de igual manera una vez finalizado el acto de apertura económico.

Visita al sitio de ejecución del contrato

La convocante dispone la realización de una visita al sitio con las siguientes indicaciones:

No Aplica

1. Difusión de la visita

La visita o inspección técnica deberá fijarse de forma previa a la fecha tope de consulta, previendo como mínimo el plazo de difusión de (02) dos días hábiles. En todos los casos, el procedimiento para su realización deberá difundirse en las bases de la contratación.

Cuando la convocante haya establecido la visita o inspección técnica, en las bases de la contratación, el oferente que conozca el sitio podrá declarar bajo fe de juramento conocer el sitio y que cuenta con la información suficiente para preparar la oferta y ejecutar el contrato.

Cuando por la naturaleza o complejidad de la contratación sea imprescindible la realización de la visita técnica, la convocante podrá establecer la obligatoriedad de dicha visita a través del SICP. En estos casos no se aceptará la presentación de la declaración jurada.

2. Desarrollo de la visita.

Se registrará en acta los asistentes, la fecha, lugar, hora de realización y funcionarios participantes. Los representantes de los oferentes que asistan a la visita podrán contar con una autorización, bastando para ello la presentación de una nota del oferente. La falta de presentación de esta autorización no impide su participación en la visita o inspección técnica.

Los gastos relacionados con dicha visita correrán por cuenta del oferente.

Incoterms

La edición de incoterms para esta licitación será:

No Aplica

Las expresiones DDP, CIP, FCA, CPT y otros términos afines, se regirán por las normas prescriptas en la edición vigente de los Incoterms publicada por la Cámara de Comercio Internacional.

Durante la ejecución contractual, el significado de cualquier término comercial, así como los derechos y obligaciones de las partes serán los prescritos en los Incoterms, a menos que sea inconsistente con alguna disposición del Contrato.

Autorización del Fabricante

Los ítems a los cuales se le requerirá Autorización del Fabricante son los indicados a continuación:

Aplica ítem 1. El Representante o Distribuidor de la marca ofertada para el ítem 1 . La carta deberá estar dirigida al convocante mencionando el ID y objeto de la licitación.

En caso de Representante o Distribuidor, éste deberá presentar las documentaciones que demuestren la cadena de autorizaciones hasta llegar al Fabricante.

Cuando la convocante lo requiera, el oferente deberá acreditarse la cadena de autorizaciones, hasta el fabricante, productor o prestador de servicios.

La autorización deberá ser presentada en idioma castellano o en su defecto acompañada de su traducción oficial, realizada por un traductor público matriculado en la República del Paraguay. Así también cada autorización debe indicar a que ítem corresponde.

Muestras

Se requerirá la presentación de muestras de los siguientes ítems y en las siguientes condiciones:

No Aplica

En caso de ser solicitadas, las muestras serán consideradas requisito indispensable para la evaluación de la oferta y deberán ser presentadas junto con la oferta, o bien en el momento y plazo fijado por la convocante en este apartado. La falta de presentación en la forma y plazo establecido por la convocante será causal de descalificación de la oferta.

Tiempo de funcionamiento de los bienes

El periodo de tiempo estimado de funcionamiento de los bienes, para los efectos de repuestos será de:

No Aplica

Plazo de reposición de bienes

El plazo de reposición de bienes para reparar o reemplazar será de:

Hasta setenta y dos (72) horas posteriores al reclamo de la Contratante y posterior a la confirmación de la recepción satisfactoria por parte del oferente adjudicado, vía correo electrónico

El proveedor garantiza que todos los bienes suministrados están libres de defectos derivados de actos y omisiones que este hubiera incurrido, o derivados del diseño, materiales o manufactura, durante el uso normal de los bienes en las condiciones que imperen en la República del Paraguay.

1. La Contratante comunicará al proveedor la naturaleza de los defectos y proporcionará toda evidencia disponible, inmediatamente después de haberlos descubierto. La contratante otorgará al proveedor facilidades razonables para inspeccionar tales defectos.

Tan pronto reciba ésta comunicación, y dentro del plazo establecido en este apartado, deberá reparar o reemplazar los bienes defectuosos, o sus partes sin ningún costo para la contratante.

2. Si el proveedor después de haber sido notificado, no cumple dentro del plazo establecido, la contratante, procederá a tomar medidas necesarias para remediar la situación, por cuenta y riesgo del proveedor y sin perjuicio de otros derechos que la contratante pueda ejercer contra el proveedor en virtud del contrato.

Periodo de validez de la Garantía de los bienes

El plazo de validez de la Garantía de los bienes será el siguiente:

El plazo de validez de la garantía es de Veinticuatro (24) meses

Cobertura de Seguro de los bienes

La cobertura de seguro requerida a los bienes será:

No Aplica

A menos que se disponga otra cosa en este apartado, los bienes suministrados deberán estar completamente asegurados en guaraníes, contra riesgo de extravío o daños incidentales ocurridos durante la fabricación, adquisición, transporte, almacenamiento y entrega, de acuerdo a los incoterms aplicables.

REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN

Esta sección contiene los criterios que la convocante utilizará para evaluar la oferta y determinar si un oferente cuenta con las calificaciones requeridas. Ningún otro factor, método o criterio será utilizado.

Condición de Participación

Podrán participar de este procedimiento, las personas físicas, jurídicas y/o Consorcio, constituidos o con acuerdo de intención, inscritos en el Registro de Proveedores del Estado.

Los oferentes domiciliados en la República del Paraguay, que pretendan participar en un procedimiento de contratación, no deberán estar comprendidos en las prohibiciones o limitaciones para presentar propuestas y contratar con el Estado, establecidas en el artículo 21 de la Ley N° 7021/22 "DE SUMINISTROS Y CONTRATACIONES PUBLICAS".

Sucursales

En los casos de procedimientos de contratación de carácter nacional podrán participar las sucursales de las matrices internacionales constituidas en la República del Paraguay. Solo serán admitidas como criterios de adjudicación las capacidades, experiencia y aptitudes de la sucursal recabadas desde su constitución, sin admitirse la utilización de las cualidades de la casa matriz u otras filiales o sucursales.

Conflicto de Interés

1. Deber de Abstención del funcionario ante un posible conflicto de interés. El funcionario público que participe en el procedimiento de contratación deberá abstenerse de intervenir, de manera directa o indirecta, en los asuntos en los que su actuación esté comprendida en alguno de los supuestos del artículo 17 de la Ley N° 7021/22. A tales efectos, deberá comunicar a su superior jerárquico o a la máxima autoridad institucional que se encuentra inmerso en uno de los supuestos legales, detallando la situación particular. En caso que corresponda, el superior jerárquico o la máxima autoridad institucional tendrá por aceptada la abstención apartando al funcionario y, de ser necesario, designará al sustituto. Se deberá dejar constancia por escrito de todo lo actuado.

2. Apartamiento del funcionario por la Entidad Convocante. Enterada la Convocante de que existe un conflicto de interés respecto a un funcionario público que ha sido designado o requerido para intervenir o que interviene en alguna de las etapas de la fase de contratación del suministro público, y no mediando la abstención expresa del funcionario, deberá apartarlo del asunto particular, detallando la situación que configura el conflicto de interés. La Convocante deberá dejar constancia por escrito de todo lo actuado. Se procederá a la designación del sustituto, en los casos que correspondiere.

3. Actuaciones tras la detección de un conflicto de interés. Si la Entidad Convocante detectare que un funcionario público comprendido en alguno de los supuestos del artículo 17 de la Ley N° 7021/22 tuvo intervención en alguna de las etapas de la fase de contratación del suministro público, adoptará las medidas que correspondan. La Convocante podrá subsanar las

actuaciones en sede administrativa o revocarlas, según corresponda. Deberá dejarse constancia por escrito de todo lo actuado y comunicarse a la DNCP. La DNCP podrá, de oficio o por denuncia fundada, realizar las investigaciones que resulten pertinentes, a fin de verificar presuntos hechos que podrían constituir conflicto de intereses y/o irregularidades en contravención con el artículo 17 de la Ley N° 7021/22, conforme las atribuciones conferidas en el artículo 132 de la Ley.

4. Declaración jurada de conocimiento de la existencia de un conflicto de intereses respecto a los funcionarios públicos intervinientes en el procedimiento. La convocante deberá verificar la “Declaración jurada de conocimiento de la existencia de un conflicto de intereses respecto a los funcionarios públicos intervinientes en el procedimiento” presentada por el oferente al momento de la oferta en cumplimiento de su obligación de comunicar o denunciar la existencia de posibles conflictos de intereses, de conformidad al artículo 17 de la Ley 7021/22. De comprobarse la omisión, falsedad o inexactitud de la información proporcionada y declarada en la Declaración la Convocante analizará si se configura un conflicto de interés en los términos del artículo 17 de la Ley 7021/22 y emitirá las directrices que correspondan acorde a la etapa del procedimiento de contratación. Además, la Convocante podrá resolver la descalificación de la oferta y/o rescisión del contrato respectivo.

Requisitos de Calificación

Calificación Legal. Los oferentes deberán declarar que no se encuentran comprendidos en las limitaciones o prohibiciones para contratar con el Estado, según lo establecido en el artículo 21 de la Ley N° 7021/22. Esta declaración forma parte del formulario de oferta.

Serán rechazadas las ofertas de los oferentes que se encuentren comprendidos en las prohibiciones o limitaciones para presentar propuesta y contratar con el Estado, a la hora y fecha límite de presentación de ofertas o a la fecha de firma del contrato.

A los efectos de la verificación de la existencia de prohibiciones o limitaciones contenidas en el artículo 21 de la Ley N° 7021/22, el comité de evaluación realizará el siguiente análisis:

1° Verificará que el oferente haya proporcionado el formulario de ofertas, el cual comprende la declaración jurada de no estar comprendido en las prohibiciones y limitaciones para presentar propuesta y contratar.

2° Además, deberá verificar la presentación de la declaración jurada de conocimiento de la existencia de un conflicto de intereses respecto a los funcionarios públicos intervinientes en el procedimiento, y de las constancias de registro de estructura jurídica y de beneficiarios finales, a fin de verificar que los oferentes no se encuentren incurso en las causales previstas en el Art 21 de la Ley N° 7021/22.

3° Verificará por los medios disponibles, si el oferente y los demás sujetos individualizados en las prohibiciones o limitaciones contenidas en los incisos d) y e) del artículo 21 de la Ley, aparecen en la base de datos del SINARH del VICE MINISTERIO DE CAPITAL HUMANO Y GESTION ORGANIZACIONAL.

4° Si se constata que alguna de las personas mencionadas en el párrafo anterior figura en la base de datos del SINARH del VICE MINISTERIO DE CAPITAL HUMANO Y GESTION ORGANIZACIONAL, el comité analizará acabadamente si tal situación le impedirá contratar con el Estado, exponiendo los motivos para aceptar o rechazar la oferta, según sea el caso.

5° Verificará que el oferente haya proporcionado el formulario de Declaración de Personas, debidamente firmado, en el Registro de Proveedores del Estado, conforme a los estándares establecidos, y cotejará los datos con las personas físicas inhabilitadas que constan en el registro de “Sanciones a Proveedores” del SICP. Con el objeto de verificar si los directores, gerentes, socios gerentes, quienes ejerzan la administración, accionistas, cuotapartistas o propietarios se encuentren dentro de los criterios contemplados en los incisos h), i), y j) de la Ley 7021/22, además la convocante se encuentra facultada de solicitar informes internos institucionales para el cotejo de la información con respecto a los incisos mencionados. La declaración jurada deberá contar con información vigente al momento de la presentación de las ofertas y el oferente será responsable de la actualización del documento que obre en el registro de proveedores del Estado. En caso de que el oferente no cuente con dicho Formulario en su registro, la Convocante procederá a solicitarlo durante la etapa de evaluación de ofertas. Si el oferente no responde el pedido o no remite el citado Formulario, se procederá al rechazo de la oferta.

6° El comité podrá recurrir a fuentes públicas o privadas de información, para verificar los datos proporcionados por el oferente y las obrantes en el registro de sancionados de la DNCP.

7° El comité verificará en fuentes públicas de información de libre acceso, si el oferente o sus integrantes, se encuentran en los demás supuestos contenidos en el artículo 21 de la Ley N° 7021/22, pudiendo utilizar como guía instructiva el

documento aprobado por la DNCP. En caso de requerirse, el comité podrá solicitar aclaración al oferente sobre la vigencia de la información obrante en las fuentes respectivas.

8° En caso de que aplique la subcontratación y que el oferente haya presentado el formulario de personas a subcontratar/subcontratadas junto con la oferta, el Comité de Evaluación de Ofertas deberá evaluar el contenido del formulario a los efectos de constatar que el subcontratista no se encuentra comprendido en alguna de las causales de prohibición previstas en el Art. 21 de la Ley N° 7021/22, pudieron requerir al oferente la información que sea necesaria.

Si el Comité confirma que el oferente o sus integrantes poseen impedimentos en virtud a lo dispuesto en el artículo 21 de la Ley N° 7021/22, la oferta será rechazada y se remitirán los antecedentes a la DNCP para los fines pertinentes.

Metodo de Evaluación

Basado únicamente en precio

Análisis de precios ofertados

Para evaluación de ofertas con el criterio basado únicamente en precio.

Luego de haber realizado la corrección de errores aritméticos y de ordenar las ofertas presentadas de menor a mayor, el Comité de Evaluación procederá a solicitar a los oferentes una explicación detallada de la composición del precio ofertado de cada ítem, rubro o partida adjudicable, conforme al siguiente parámetro:

En contrataciones en general: cuando la diferencia entre el precio ofertado y el precio referencial sea superior al 25% para ofertas por debajo del precio referencial y del 15% para ofertas que se encuentren por encima del referencial establecido por la convocante y difundido con el llamado a contratación.

Si el oferente no respondiese la solicitud, o la respuesta no sea suficiente para justificar el precio ofertado del bien o servicio, el precio será declarado inaceptable y la oferta rechazada.

El análisis de los precios, con esta metodología, será aplicado a cada ítem, rubro o partida que componga la oferta y en cada caso deberá ser debidamente fundada la decisión adoptada por la Convocante en el ejercicio de su facultad discrecional.

Para la evaluación de ofertas basada en la multiplicidad de criterios.

En cuanto al análisis del precio se podrá considerar el parámetro dispuesto en el presente apartado.

Composición de Precios

La estructura mínima del desglose de composición de los precios, será:

bien/servicio ofertado.	Costo expresado en la moneda de la oferta.
Elementos de Valor Fijo	
Mano de obra	
Inmuebles	
Maquinarias	
Herramientas	
Vehículos	
Equipos informáticos	
Muebles	
Seguros	
Servicios básicos	
Elementos de Valor Variable	
Insumos	
Mantenimiento	
Gastos administrativos	
Gastos de venta	
Total de costos	
Utilidad esperada	
Precio del bien/servicio antes de impuestos	

Impuestos

Precio final del bien/servicio impuestos incluidos

El oferente podrá presentar junto con su oferta el desglose de composición de precios, cuando su oferta se encuentre fuera de los parámetros establecidos en la cláusula anterior.

Cuando la Convocante requiera el desglose con el propósito de facilitar el análisis y comparación de las ofertas, el oferente deberá ajustarse a la estructura mínima establecida y, en caso de considerarlo pertinente, podrá complementarla e incluir una explicación detallada o parámetros que permitan aclarar aspectos puntuales de su composición y/o sustentar la razonabilidad de sus precios.

Certificado de Producto y Empleo Nacional - CPS

a) Oferentes. A los efectos de acogerse al beneficio de la aplicación del margen de preferencia, el oferente deberá contar con el Certificado de Producto y Empleo Nacional (CPEN). El certificado debe ser emitido como máximo a la fecha y hora tope de presentación de ofertas. La falta del CPEN no será motivo de descalificación de la oferta, sin embargo, el oferente no podrá acogerse al beneficio.

El comité de evaluación verificará en el portal oficial indicado por el Ministerio de Industria y Comercio (MIC) la emisión en tiempo y forma del CPEN declarado por los oferentes. No será necesaria la presentación física del Certificado de Producto y Empleo Nacional.

Independientemente al sistema de adjudicación, el margen de preferencia será aplicado a cada bien o servicio objeto de contratación que se encuentre indicado en la planilla de precios.

El CPEN será intransferible, no obstante, exclusivamente en caso de productos y bajo autorización expresa del titular del certificado, éste podrá ser utilizado por terceros para la presentación de ofertas en el marco de un procedimiento de contratación, de acuerdo con lo establecido en la reglamentación respectiva.

b) Oferentes en Consorcio:

b.1. Provisión de Bienes. El CPEN debe ser expedido a nombre del oferente que fabrique o produzca los bienes objeto de la contratación. En el caso que ninguno de los oferentes consorciados fabrique o produzca los bienes ofrecidos, el consorcio deberá contar con el CPEN correspondiente al bien ofertado, debiendo encontrarse debidamente autorizado por el fabricante. Esta autorización podrá ser emitida a nombre del consorcio o de cualquiera de los integrantes del mismo.

b.2. Provisión de Servicios. (se entenderá por el término “servicio” aquello que comprende a los servicios en general, las consultorías, obras públicas y servicios relacionados a obras públicas).

Todos los integrantes del consorcio deben contar con el CPEN.

Excepcionalmente se admitirá que no todos los integrantes del consorcio cuenten con el CPEN para aplicar el margen de preferencia, cuando el servicio específico se encuentre detallado en uno de los ítems de la planilla de precios, y de los documentos del consorcio (acuerdo de intención o consorcio constituido) se desprenda que el integrante del consorcio que cuenta con el CPEN será el responsable de ejecutar el servicio licitado

Requisitos documentales para la evaluación de las condiciones de participación.

1. Formulario de Oferta (*) <i>[El formulario de oferta y lista de precios, generados electrónicamente a través del SICP, deben ser completados y firmados por el oferente. En caso de que se emplee el módulo de oferta electrónica se considerará que el listado de ítems forma parte del formulario de oferta electrónica, y deberá sujetarse en todo lo demás a la reglamentación vigente.]</i>
2. Garantía de Mantenimiento de Oferta (*) <i>[La garantía de mantenimiento de oferta debe ser extendida, bajo la forma establecida en el SICP.]</i>
3. Certificado de Cumplimiento con la Seguridad Social (**)
4. Declaración jurada de conocimiento de la existencia de un conflicto de intereses respecto a los funcionarios públicos intervinientes en el procedimiento. (**)
5. Certificado de Producto y Empleo Nacional emitido por el MIC, en formato físico, solo en caso de imposibilidad de certificación electrónica. (**)
6. Certificado de Cumplimiento Tributario. (**)
7. Patente comercial del municipio en donde esté asentado el establecimiento del oferente. (**)
8. Documentos legales. Oferentes
8.1. Personas Físicas.
a. Fotocopia simple de la Cédula de Identidad del firmante de la oferta. (*)
b. Constancia de inscripción en el Registro Único de Contribuyentes – RUC (*)
c. En el caso que suscriba la oferta otra persona en su representación, deberá acompañar una fotocopia simple de su cédula de identidad y una fotocopia simple del poder suficiente otorgado por Escritura Pública para presentar la oferta y representarlo en los actos de la licitación. No es necesario que el poder esté inscripto en el Registro de Poderes. (*)

8.2. Personas Jurídicas.
a. Fotocopia simple de los documentos que acrediten la existencia legal de la persona jurídica tales como la Escritura Pública de Constitución, según el tipo de sociedad y protocolización de los Estatutos Sociales. Los estatutos deberán estar inscriptos en la Sección Personas Jurídicas de la Dirección de Registros Públicos. (*)
b. Constancia de inscripción en el Registro Único de Contribuyentes. (**)
c. Fotocopia simple de los documentos de identidad de los representantes o apoderados de la sociedad. (*)
d. Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al oferente. Estos documentos pueden consistir en: un poder suficiente en el que conste que el apoderado posee facultades suficientes para representar y obligar a la persona jurídica, otorgado por Escritura Pública (no es necesario que esté inscripto en el Registro de Poderes); o los documentos societarios que justifiquen la representación del firmante, tales como las actas de asamblea y de directorio en el caso de las sociedades anónimas. (*)
8.3. Oferentes en Consorcio en formación.
a. Original o fotocopia del acuerdo de intención de constituir el consorcio, en caso de resultar adjudicados y antes de la firma del contrato. (*)
b. Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al consorcio en formación y que acrediten las facultades de los firmantes del acuerdo de intención para consorciarse. Estos documentos pueden consistir en (*): I. Original o fotocopia del acuerdo de intención de constituir el consorcio en caso de resultar adjudicados y antes de la firma del contrato, instrumentado por escritura pública, o II. Original o fotocopia del acuerdo de intención de constituir el consorcio en caso de resultar adjudicados y antes de la firma del contrato, instrumentado por acuerdo privado. Cada integrante del consorcio que sea persona física domiciliada en la República del Paraguay deberá presentar los documentos requeridos para Oferentes Individuales especificados en el apartado Oferentes. (Personas Físicas) y, las personas jurídicas domiciliadas en Paraguay deberán presentar los documentos requeridos para Oferentes (Personas Jurídicas).
c. Un poder en el que conste que el apoderado posee facultades suficientes para representar y obligar al Consorcio, otorgado por escritura pública (no es necesario que esté inscripto en el Registro de Poderes) (*).
8.4. Oferentes en Consorcios constituidos o formalizados.

a. Original o fotocopia del instrumento público (escritura pública) de constitución del consorcio. (*)

b. Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al consorcio. Estos documentos pueden consistir en (*):

- i. Original o fotocopia del instrumento público (escritura pública) de constitución del consorcio.
- ii. Un poder en el que conste que el apoderado posee facultades suficientes para representar y obligar al Consorcio, otorgado por escritura pública (no es necesario que esté inscripto en el Registro de Poderes).

Las formalidades de los acuerdos de intención y de los consorcios serán determinadas por la Dirección Nacional de Contrataciones Públicas (DNCP).

En caso de que los procedimientos no sean por el módulo de oferta electrónica, el oferente deberá presentar el Formulario de Oferta y la Planilla de precio. Para los casos en que se utilice el Módulo de Oferta Electrónica los datos se deberán cargar en el Formulario de oferta electrónica de conformidad a la normativa vigente.

Los documentos indicados con asterisco (*) son considerados documentos sustanciales a ser presentados con la oferta de conformidad al Decreto Reglamentario.

Los documentos indicados con doble asterisco (**) deberán estar vigentes a la fecha y hora tope de presentación de ofertas. La falta de firma en documentos formales no será un motivo de descalificación, salvo que expresamente se disponga la exigencia de la firma del oferente, en cuyo caso la omisión o desconformidad deberá analizarse conforme a los Artículos 77, 78 y 80 del Decreto 2264/24.

Respecto al punto 3, cuando el oferente se encuentre activo sin movimiento, deberá presentar la documentación respaldatoria expedida por autoridad competente. En caso de no contar con personal subordinado por tratarse de un consultor individual, el oferente deberá presentar el certificado de no hallarse inscripto en el IPS.

Capacidad Financiera

Con el objetivo de calificar la situación financiera del oferente, se considerarán los siguientes índices:

a) Para contribuyente de IRE GENERAL.

Deberán cumplir el siguiente parámetro:

a. **Ratio de Liquidez:** activo corriente / pasivo corriente.

Deberá ser igual o mayor que 1.5, en promedio, de los 3 años (2022, 2023 y 2024).

b. **Endeudamiento:** pasivo total / activo total.

No deberá ser mayor a 0,65 en promedio, de los 3 años (2022, 2023 y 2024).

c. **Rentabilidad:** Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital.

El promedio de los 3 años deberá ser igual o superior al 10% (2022, 2023 y 2024).

Observación: Si en alguno de los tres años, o los tres años presentados por la Empresa, su pasivo es igual a 0, se considerará el Ratio de Liquidez igual a 1.5 y se dará por cumplido el Ratio de Endeudamiento. Esta salvedad en el PBC hace posible calcular el promedio del índice de liquidez de los 3 (tres) ejercicios analizados, debido a que se otorga un valor que puede ser promediado.

b) Para contribuyente de IRE SIMPLE.

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso):

Deberá ser igual o mayor que 1.3, en promedio, de los 3 años (2022, 2023 y 2024).

c) Para contribuyente de IRP.

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1.3, en promedio, de los 3 años (2022, 2023 y 2024).

d) Para contribuyentes de exclusivamente IVA General.

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1.3, en promedio, de los 3 años (2022, 2023 y 2024).

Los oferentes al efecto de lo anteriormente señalado, deberán presentar los documentos que se indican en los requisitos documentales

Observación: En Caso de Oferentes en Consorcio, el Oferente Líder del Consorcio deberá cumplir con la capacidad financiera mínima requerida.

Requisitos documentales para la evaluación de la capacidad financiera

Para evaluar el presente criterio, el oferente deberá presentar las siguientes documentaciones:

a. Balance General y Cuadro de Estado de Resultados de los años 2022, 2023 y 2024 para contribuyente de IRE General.
b. Formulario 106 de los años 2022, 2023 y 2024 para contribuyentes del IRE Simple.
c. Formulario 104 de los años 2022, 2023 y 2024 para contribuyentes de Renta Personal.
d. IVA General de 36 (treinta y seis) meses de los años 2022, 2023 y 2024 según la Circular N° 11/2020 y las demás reglamentaciones vigentes de la DNIT, para contribuyentes sólo del IVA General.

Experiencia requerida

Con el objetivo de calificar la experiencia del oferente, se considerarán los siguientes índices:

- a. Demostrar experiencia en servicios de diseño, implementación y operación de SOC. Para lo propio, se considerará dicha experiencia por medio de la presentación de contratos, facturas y actas de recepción final (enunciación taxativa). Los servicios mencionados podrán corresponder tanto a instituciones públicas como privadas en la República del Paraguay y haber sido ejecutados dentro del periodo de los últimos tres ejercicios contables (período comprendido entre los años 2022,2023,2024).

El resultado de la suma de los montos de los contratos y/o facturaciones de venta deberá ser igual o superior al cincuenta por ciento (50%) del monto total ofertado.

- b. Demostrar experiencia en contratos de similares características, resultados esperados y KPIs:
 - i. Tiempo medio de detección (MTTD) de incidentes: < 30 minutos.
 - ii. Tiempo medio de respuesta (MTTR) a incidentes críticos: < 2 horas.
 - iii. Porcentaje de falsos positivos: < 10%.
 - iv. Tiempo de inactividad no planificado debido a incidentes de seguridad: < 0.1%.
 - v. Porcentaje de vulnerabilidades críticas remediadas dentro del SLA: >80%.
 - vi. Número de amenazas proactivamente identificadas a través de threat hunting: > 2 por mes.
 - vii. Tasa de éxito en la contención de incidentes: > 90%

Observación: *La convocante se reserva el derecho de solicitar documentación respaldatoria referida al inc b). *En consorcios, todos los integrantes deben cumplir la experiencia mínima requerida.

La actividad comercial, industrial o de servicios debe estar vinculada con el tipo de bienes o servicios a contratar.

Requisitos documentales para la evaluación de la experiencia

1. Copia de facturas, contratos y recepciones finales y/o *Declaración jurada*.

Se deberá acreditar que el giro comercial de la empresa corresponde al procedimiento de contratación ofertado, para lo cual deberá presentar copia simple y legible del documento que acredite la actividad comercial, industrial o de servicio, pudiendo ser: la constancia de RUC, patente municipal o documentos constitutivos, siempre que de la documentación se desprenda su actividad comercial y la correspondencia al procedimiento objetado. Cuando no resulte aplicable la constancia de RUC o la patente municipal, el oferente deberá manifestar y justificar esta condición en su oferta y presentar otra documentación a los efectos de acreditar el giro comercial.

Capacidad Técnica

El oferente deberá proporcionar evidencia documentada que demuestre su cumplimiento con los siguientes requisitos de capacidad técnica:

Infraestructura Local y Centro de Operaciones

- a. Domicilio legal y SOC en territorio Paraguayo: El oferente deberá contar con una oficina operativa con domicilio legal en la República del Paraguay y un Centro de Operaciones de Seguridad (SOC) activo, operativo al momento de la presentación de la oferta.

b. Características mínimas del SOC:

- Monitoreo continuo (24x7) de eventos de seguridad.
- Capacidad para gestionar como mínimo 1.000 activos (endpoints o servidores).
- Registro comercial vigente (patente municipal).
- Declaración jurada detallando: número de activos monitoreados, volumen aproximado de logs procesados por día, herramientas y plataformas utilizadas.

c. Evidencia de Operación del SOC: Presentar al menos tres (3) certificados o constancias contractuales que acrediten la operación del SOC durante los últimos 12 meses.

Personal Técnico Requerido

a. Técnicos de Monitoreo SOC: Al menos cuatro (4) técnicos con experiencia mínima de 2 años en ciberseguridad. Estos deben figurar en la planilla IPS del mes anterior vencido.

b. Coordinador Técnico: Un (1) coordinador con experiencia mínima de dos (2) años, registrado en IPS, con las siguientes funciones:

- - Representar un nexo con la entidad contratante.
- - Supervisar procedimientos de monitoreo.
- - Presentar informes mensuales.

Perfiles y Certificaciones del Personal

Rol	Cantidad	Requisitos Exigidos	Experiencia General	Experiencia Específica	Exigido
Líder de Proyecto	1	- Licenciatura en Análisis de Sistemas o Ingeniería Informática. - Certificación en Gestión de Riesgos - Certificación en Auditoría de Sistemas y/o Seguridad de la Información. - Certificación en Auditoría ISO/IEC 27001 (40hs o más). - Certificación en Seguridad de Información y/o Continuidad de Negocio (100 o más horas).	5 años en seguridad de la información	3 años en gestión de proyectos de seguridad de la información y auditorías ISO 27001	

Implementación de Solución	1	- Licenciatura en Análisis de Sistemas o Ingeniería Informática. - Curso administración servidores - Certificación de Auditor Interno ISO 27001:2022 - Curso MGCTI y/o SCRUM y/o Seguridad de la información - Diplomado en Ciberseguridad y/o Hacking Ético 80h - Certificación en Analista SOC - Certificaciones de ciberseguridad como FCA, FCF, Cisco Cybersecurity.	5 años en implementación de soluciones	3 años en configuración de servidores, controles ISO 27001, despliegue de herramientas	
Soporte Ciberseguridad	1	- Estudiante/Egresado Análisis de Sistemas/Ingeniería Informática - Certificación en solución ofertada - Curso de Ciberseguridad o Hacking Ético de mínimo 70 horas. - Manejo de firewalls, IPS/IDS, VPN - Experiencia con DLP/SIEM - Experiencia en implementación de los Controles Críticos de Ciberseguridad NIST - Experiencia en la realización de Pentesting (Caja Negra, Caja Gris y Caja Blanca) - Experiencia como instructor en ciberseguridad	5 años en soporte ciberseguridad	3 años en firewalls, IPS/IDS, VPN, SIEM, NIST, pentesting	

Soporte y Monitoreo SOC	2	- Estudiante o egresado de Análisis de Sistemas, Ingeniería Informática o afines.- Certificación avanzada solución ofertada - Curso de redes - Certificación CCNA en ciberseguridad, seguridad de la información o equivalente. - 2 años en ciberseguridad - Estos técnicos deben formar parte del plantel de la empresa y figurar en la planilla del Instituto de Previsión Social (IPS) correspondiente al mes anterior vencido a la fecha de la etapa competitiva.	2 años en soporte ciberseguridad	1 año en monitoreo SOC (análisis de logs, respuesta a incidentes)	
-------------------------	---	---	----------------------------------	---	--

Observación:

En caso de Oferentes en Consorcio, todos los integrantes del Consorcio deberán cumplir la capacidad técnica mínima requerida.

Requisitos documentales para evaluar el criterio de capacidad técnica

Los siguientes documentos serán los considerados para la evaluación del presente criterio:

a. Copia de patente comercial vigente de la oficina operativa en Paraguay. 2. Planilla del IPS del mes anterior vencido para técnicos y coordinador técnico.
b. Declaración jurada detallando: número de activos monitoreados, volumen aproximado de logs procesados por día, herramientas y plataformas utilizadas.
c. Al menos tres (3) certificados o constancias contractuales o cartas de referencia que acrediten la operación del SOC durante los últimos 12 meses.

- d. Presentar copia de planilla de IPS y/o contrato de los perfiles solicitados, acompañado del respectivo Currículum Vitae, certificados de capacitaciones y/o constancias que avalen la experiencia para cada perfil

Aclaración de las ofertas

Con el objeto de realizar la revisión, evaluación, comparación y posterior calificación de ofertas, el Comité de Evaluación podrá solicitar a los oferentes, aclaraciones respecto de sus ofertas, dichas solicitudes y las respuestas de los oferentes se realizarán por escrito.

A los efectos de confirmar la información o documentación suministrada por el oferente, el Comité de Evaluación, podrá solicitar aclaraciones a cualquier fuente pública o privada de información.

Las aclaraciones de los oferentes que no sean en respuesta a aquellas solicitadas por la convocante, no serán consideradas.

No se solicitará, ofrecerá, ni permitirá ninguna modificación a los precios ni a la sustancia de la oferta, excepto para confirmar la corrección de errores aritméticos.

El comité de evaluación podrá solicitar aclaración respecto al CPEN, cuando se deba a omisiones o errores formales en la lista de precio, debiendo el oferente limitarse a responder a la solicitud de aclaración remitiendo el formulario respectivo anexo al Pliego.

Disconformidades, errores y omisiones

Siempre y cuando una oferta se ajuste sustancialmente a las bases de la contratación, el Comité de Evaluación, requerirá que cualquier disconformidad u omisión que no constituya una desviación significativa, sea subsanada en cuanto a la información o documentación que permita al Comité de Evaluación realizar la calificación de la oferta.

A tal efecto, el Comité de Evaluación emplazará por escrito al oferente a que presente la información o documentación necesaria, dentro de un plazo razonable no menor a un día hábil, bajo apercibimiento de rechazo de la oferta. El Comité de Evaluación podrá reiterar el pedido cuando la respuesta no resulte satisfactoria, toda vez que no se viole el principio de igualdad.

Con la condición de que la oferta cumpla sustancialmente con los Documentos de la Licitación, la convocante corregirá errores aritméticos de la siguiente manera y notificará al oferente para su aceptación:

- a) Si hay una discrepancia entre un precio unitario y el precio total obtenido al multiplicar ese precio unitario por las cantidades correspondientes, prevalecerá el precio unitario y el precio total será corregido.
- b) Si hay un error en un total que corresponde a la suma o resta de subtotales, los subtotales prevalecerán y se corregirá el total.
- c) En caso que el oferente haya cotizado su precio en moneda extranjera con décimos y céntimos la convocante procederá a realizar el redondeo hacia abajo.

Si hay una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras a menos que la cantidad expresada en palabras corresponda a un error aritmético, en cuyo caso prevalecerán las cantidades en cifras de conformidad con los párrafos (a) y (b) mencionados.

Criterios de desempate de ofertas

En caso de que existan dos o más oferentes solventes que cumplan con todos los requisitos establecidos en el pliego de bases y condiciones del procedimiento de contratación, igualen en precio y sean sus ofertas las más bajas, el comité de evaluación determinará cuál de ellas es la mejor calificada para ejecutar el contrato utilizando los criterios dispuestos para el efecto por la DNCP en la reglamentación pertinente.

Criterios de Adjudicación

De acuerdo con el mercado, el objeto del contrato y el ciclo de vida del bien o servicio, podrá usarse uno o la combinación de varios criterios, previstos en el artículo 52 de la Ley N° 7021/22 “De Suministro y Contrataciones Públicas”.

La adjudicación de la oferta solo podrá fundamentarse en la evaluación de los criterios señalados en los documentos del procedimiento de contratación.

En los procedimientos de contratación en los cuales se aplique la combinación de criterios, la evaluación de las ofertas se llevará a cabo con base a la metodología, criterios y parámetros establecidos en los pliegos de bases y condiciones que permitan establecer cuál es aquella que ofrece mayor valor por dinero.

En los demás casos, la convocante adjudicará el contrato al oferente cuya oferta haya sido evaluada como la más baja y cumpla sustancialmente con los requisitos de las bases y condiciones, siempre y cuando la convocante determine que el oferente está calificado para ejecutar el contrato satisfactoriamente.

1. La adjudicación en los procedimientos de contratación en los cuales se aplique el atributo de contrato abierto, se efectuará por las cantidades o montos máximos solicitados en el procedimiento de contratación, sin que ello implique obligación de la convocante de requerir la provisión de esa cantidad o monto durante de la vigencia del contrato, obligándose sí respecto de las cantidades o montos mínimos establecidos.

2. En caso de que la convocante no haya adquirido la cantidad o monto mínimo establecido, deberá consultar al proveedor si desea ampliarlo para el siguiente ejercicio fiscal, hasta cumplir el mínimo.

3. Al momento de adjudicar el contrato, la convocante se reserva el derecho a disminuir la cantidad de Bienes y/o Servicios requeridos, por razones de disponibilidad presupuestaria u otras razones debidamente justificadas. Estas variaciones no podrán alterar los precios unitarios u otros términos y condiciones de la oferta y de los documentos de la licitación.

En aquellos procedimientos de contratación en los cuales se aplique el atributo de contrato abierto, cuando la Convocante deba disminuir cantidades o montos a ser adjudicados, no podrá modificar el monto o las cantidades mínimas establecidas en las bases de la contratación.

Notificación del resultado

La notificación del resultado se realizará a través del SICP de manera automática, desde la publicación de los documentos en el SICP, a los correos declarados en el Registro de Proveedores del Estado de los oferentes presentados. A efectos de la notificación oficial, solo serán considerados tales correos electrónicos. Dicha notificación, al tiempo de la publicación de los documentos en el SICP, comprenderá la Resolución del resultado de la adjudicación y el informe de evaluación

respectivo.

En casos excepcionales regulados por la DNCP, las Convocantes podrán dar a conocer el resultado por otros medios físicos o electrónicos a cada uno de los oferentes, remitiendo junto a la notificación, la copia íntegra de la resolución de adjudicación y del informe de evaluación, de conformidad al artículo 82 del Decreto.

En caso de que la convocante opte por la notificación física a los oferentes participantes, ésta deberá contar con la mención de haberse acompañado el informe de evaluación y la resolución de adjudicación correspondientes y con el acuse de recibo. De no contar con este último, se considerará que la notificación fue realizada en la fecha de publicación de los documentos relativos al resultado en el SICP.

En caso de que la convocante opte por la notificación por correo electrónico, se considerará que el oferente ha sido debidamente notificado desde el día siguiente de la notificación, en consecuencia, no se requerirá del acuse de recibo por parte del oferente.

La solicitud del Informe de Evaluación suspende el plazo para formular protestas hasta tanto la convocante haga entrega de dicha copia al oferente solicitante.

Las cancelaciones o declaraciones desiertas deberán ser notificadas a todos los oferentes, según el procedimiento indicado precedentemente.

Las notificaciones realizadas en virtud al contrato, deberán ser por escrito y dirigirse a la dirección indicada en el contrato.

Audiencia Informativa

Una vez notificado el resultado del proceso, el oferente tendrá la facultad de solicitar una audiencia a fin de que la convocante explique los fundamentos que motivan su decisión.

La solicitud de audiencia informativa no suspenderá ni interrumpirá el plazo para la interposición de protestas.

El procedimiento de realización de la misma deberá ajustarse a las reglamentaciones vigentes para el efecto.

SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS

Esta sección constituye el detalle de los bienes con sus respectivas especificaciones técnicas - EETT, de manera clara y precisa para que el oferente elabore su oferta. Salvo aquellas EETT de productos ya determinados por plantillas aprobadas por la DNCP.

Suministros y Especificaciones técnicas

Esta sección constituye el detalle de los bienes y/o servicios con sus respectivas especificaciones técnicas - EETT, de manera clara y precisa para que el oferente elabore su oferta. Salvo aquellas EETT de productos ya determinados por plantillas aprobadas por la DNCP.

El Suministro deberá incluir todos aquellos ítems que no hubiesen sido expresamente indicados en la presente sección, pero que pueda inferirse razonablemente que son necesarios para satisfacer el requisito de suministro indicado, por lo tanto, dichos bienes y servicios serán suministrados por el Proveedor como si hubiesen sido expresamente mencionados, salvo disposición contraria en el Contrato.

Los bienes y servicios suministrados deberán ajustarse a las especificaciones técnicas y las normas estipuladas en este apartado. En caso de que no se haga referencia a una norma aplicable, la norma será aquella que resulte equivalente o superior a las normas oficiales de la República del Paraguay. Cualquier cambio de dichos códigos o normas durante la ejecución del contrato se aplicará solamente con la aprobación de la contratante y dicho cambio se registrará de conformidad a la cláusula de adendas y convenios modificatorios.

El Proveedor tendrá derecho a rehusar responsabilidad por cualquier diseño, dato, plano, especificación u otro documento, o por cualquier modificación proporcionada o diseñada por o en nombre de la Contratante, mediante notificación a la misma de dicho rechazo.

Identificación de la unidad solicitante y justificaciones

En este apartado la convocante deberá indicar los siguientes datos:

- Ingeniero. Eder Atilio Añazco Greco, Director de la Dirección de Tecnología de la Información y comunicación

- **JUSTIFICACIÓN DEL PROYECTO:**

La creciente sofisticación de ciberamenazas, como intrusiones, malware y accesos no autorizados, pone en riesgo la infraestructura tecnológica de la institución, que incluye redes corporativas, servidores y más de 1000 endpoints. La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001 y un Centro de Operaciones de Seguridad (SOC) con herramientas mixtas propietarias y de código abierto es técnicamente necesaria para detectar y mitigar problemas de seguridad en tiempo real, garantizando la confidencialidad, integridad y disponibilidad de la información, y cumpliendo con los objetivos estratégicos de la institución.

OBJETIVO GENERAL:

Fortalecer la capacidad de prevención, detección y minimización de intrusiones en la red de la institución.

OBJETIVOS ESPECÍFICOS:

- Detectar mediante firmas o patrones de comportamiento intrusiones o intentos.
- Activamente establecer reglas de bloqueo en caso de detectar anomalías en la red.
- Responder de forma correcta incidentes de ciberseguridad.

- Mejora continua

RESULTADOS ESPERADOS:

- Equipo de seguridad instalado, en funcionamiento y con detección de intrusiones configurada.
- Reducción del tiempo medio de detección (MTTD) a ≤ 60 minutos y del tiempo medio de respuesta (MTTR) en un 70% para el mes 7.
- Resolución de incidentes críticos en ≤ 24 horas.
- Infraestructura protegida con herramientas escalables de código abierto (Wazuh, TheHive, osTicket).
- Personal técnico capacitado y colaboradores sensibilizados, garantizando autonomía operativa.

1. JUSTIFICACIÓN TÉCNICA

1.1. Protección de Infraestructura Crítica

La organización gestiona redes corporativas, servidores y más de 1000 endpoints, los cuales son vulnerables a amenazas como malware, explotación de vulnerabilidades y accesos no autorizados. Un SGSI basado en ISO/IEC 27001 permitirá establecer controles robustos para mitigar riesgos, mientras que el SOC, proporcionará monitoreo continuo y respuesta rápida a incidentes, reduciendo el tiempo medio de detección (MTTD) a ≤ 60 minutos y el tiempo medio de respuesta (MTTR) en un 70% para el mes 12.

2.2. Cumplimiento Normativo y del Pliego

El proyecto asegura la conformidad con el pliego de bases y condiciones, implementando políticas alineadas con ISO 27001, NIST CSF y CIS Controls. Las auditorías semestrales y la matriz de riesgos garantizarán el cumplimiento continuo.

2.3. Respuesta Efectiva a Incidentes

La formación en ciberseguridad con roles definidos (coordinador, analista, forense) y playbooks específicos para ransomware, phishing y DDoS permitirá una respuesta estructurada y eficiente. La integración de feeds de inteligencia de amenazas en el SOC mejorará la detección proactiva, mientras que simulaciones de incidentes fortalecerán la preparación del equipo.

2.4. Escalabilidad y Sostenibilidad

El uso de herramientas de código abierto asegura escalabilidad sin costos recurrentes de licenciamiento. Estas herramientas, combinadas con herramientas propietarias garantizan la continuidad del servicio durante los 24 meses del proyecto y más allá.

2.5. Fortalecimiento de Capacidades

La capacitación técnica de 300 horas para 2 técnicos en herramientas y análisis de vulnerabilidades, junto con la sensibilización gamificada, asegura la transferencia de conocimiento y la adopción de una cultura de ciberseguridad.

2.6. Reducción de Riesgos Operativos

El diagnóstico inicial con auditorías CIS, OWASP Top 10 identificará vulnerabilidades críticas, permitiendo priorizar su mitigación. La optimización de reglas de detección reducirá falsos positivos, mejorando la eficiencia del SOC. Además, la garantía de 24 meses y el soporte post-implementación aseguran la estabilidad operativa.

3. BENEFICIOS ESPERADOS

- **Seguridad Reforzada:** Protección de la confidencialidad, integridad y disponibilidad de la información en redes y endpoints.
- **Cumplimiento Normativo:** Alineación con ISO 27001 y el pliego de bases, con auditorías que validan el cumplimiento.
- **Respuesta Ágil:** Reducción de MTTD y MTTR, con resolución de incidentes críticos en ≤ 24 horas.
- **Sostenibilidad:** Uso de herramientas de código abierto para minimizar costos a largo plazo.
- **Capacitación Efectiva:** Equipo interno capacitado y colaboradores sensibilizados, reduciendo errores humanos.
- **Autonomía:** Transferencia de conocimiento completa para la operación independiente del SOC y SGSI.

Los productos y/o servicios a ser requeridos cuentan con las siguientes especificaciones técnicas:

El propósito de la Especificaciones Técnicas (EETT), es el de definir las características técnicas de los bienes que la convocante requiere. La convocante preparará las EETT detalladas teniendo en cuenta que:

- Las EETT sirven de referencia para verificar el cumplimiento técnico de las ofertas y posteriormente evaluarlas. Por lo tanto, unas EETT bien definidas facilitarán a los oferentes la preparación de ofertas que se ajusten a los documentos de licitación, y a la convocante el examen, evaluación y comparación de las ofertas.
- En las EETT se deberá estipular que todos los bienes o materiales que se incorporen en los bienes deberán ser nuevos, sin uso y del modelo más reciente o actual, y que contendrán todos los perfeccionamientos recientes en materia de diseño y materiales, a menos que en el contrato se disponga otra cosa.
- En las EETT se utilizarán las mejores prácticas. Ejemplos de especificaciones de adquisiciones similares satisfactorias en el mismo sector podrán proporcionar bases concretas para redactar las EETT.
- Las EETT deberán ser lo suficientemente amplias para evitar restricciones relativas a manufactura, materiales, y equipo generalmente utilizados en la fabricación de bienes similares.
- Las normas de calidad del equipo, materiales y manufactura especificadas en los Documentos de Licitación no deberán ser restrictivas. Se deberán evitar referencias a marcas, números de catálogos u otros detalles que limiten los materiales o artículos a un fabricante en particular. Cuando sean inevitables dichas descripciones, siempre deberá estar seguida de expresiones tales como “o sustancialmente equivalente” u “o por lo menos equivalente”, remitiendo la aclaración respectiva. Cuando en las ET se haga referencia a otras normas o códigos de práctica particulares, éstos solo serán aceptables si a continuación de los mismos se agrega un enunciado indicando otras normas emitidas por autoridades reconocidas que aseguren que la calidad sea por lo menos sustancialmente igual.
- Asimismo, respecto de los tipos conocidos de materiales, artefactos o equipos, cuando únicamente puedan ser caracterizados total o parcialmente mediante nomenclatura, simbología, signos distintivos no universales o marcas, únicamente se hará a manera de referencia, procurando que la alusión se adecue a estándares internacionales comúnmente aceptados.
- Las EETT deberán describir detalladamente los siguientes requisitos con respecto a por lo menos lo siguiente:
 - (a) Normas de calidad de los materiales y manufactura para la producción y fabricación de los bienes.
 - (b) Lista detallada de las pruebas requeridas (tipo y número).
 - (c) Otro trabajo adicional y/o servicios requeridos para lograr la entrega o el cumplimiento total.
 - (d) Actividades detalladas que deberá cumplir el proveedor, y consiguiente participación de la convocante.
 - (e) Lista detallada de avals de funcionamiento cubiertas por la garantía, y las especificaciones de las multas aplicables en caso de que dichos avals no se cumplan.
- Las EETT deberán especificar todas las características y requisitos técnicos esenciales y de funcionamiento, incluyendo los valores máximos o mínimos aceptables o garantizados, según corresponda. Cuando sea necesario, la convocante deberá incluir un formulario específico adicional de oferta (como un Anexo a la de Oferta), donde el oferente proporcionará la información detallada de dichas características técnicas o de funcionamiento con relación a los valores aceptables o garantizados.

Cuando la convocante requiera que el oferente proporcione en su oferta datos sobre una parte de o todas las Especificaciones Técnicas, cronogramas técnicos, u otra información técnica, la convocante deberá detallar la información requerida y la forma en que deberá ser presentada por el oferente en su oferta.

Si se debe proporcionar un resumen de las EETT, la convocante deberá insertar la información en la tabla siguiente. El oferente preparará un cuadro similar para documentar el cumplimiento con los requerimientos.

Detalle de los bienes y/o servicios

Los bienes y/o servicios deberán cumplir con las siguientes especificaciones técnicas y normas:

Ítem 1 - Servicio de Monitoreo y Remediación de Vulnerabilidades para 700 Dispositivos por 2 Años

N°	Descripción del Requerimiento	Exigido
PLATAFORMAS		
	La plataforma debe ser Cloud - SaaS	Sí
	La plataforma debe ser fácil de usar y navegar (usabilidad intuitiva)	Si
	La plataforma debe tener una arquitectura escalable	Sí
	La plataforma debe soportar alta disponibilidad	Sí
	La plataforma debe permitir instalar un proxy en la red para patching y caching	Sí
	El proxy debe ejecutarse en sistemas Linux Ubuntu o Red Hat	Sí
	El proxy no debe tener costo adicional	Sí
CARACTERÍSTICAS		
	Actualizar los servidores sin interrumpir el servicio	Sí
	La plataforma debe soportar los sistemas operativos más comunes (Windows, Linux y Mac)	Si
	Modelo compliance debe poder generar estadísticas de cumplimiento.	Si
	Evaluación continua de vulnerabilidades	Sí
	Reconocimiento automático de aplicaciones	Sí
	Priorización de amenazas basada en activos	Sí
	Priorización de vulnerabilidades con inteligencia interna	Sí
	Priorización de superficies de vulnerabilidades descubiertas	Sí

	Proceso de clasificación de riesgos para priorizar la corrección de vulnerabilidades descubiertas	Sí
	Clasificación de riesgo basada en activos	Sí
	Clasificación de riesgo por aplicaciones	Sí
	Presentar la clasificación de riesgo y priorizar las vulnerabilidades a corregir en orden de criticidad, considerando no solo CVE, sino también el contexto de desempeño y la situación del entorno	Sí
	Mapeo de priorización	Sí
	Administración de parches para Windows OS	Sí
	Administración de parches para aplicaciones de terceros en Windows	Sí
	Administración de parches para aplicaciones de terceros en Linux	Sí
	Poseer un módulo de vulnerabilidad para descubrimiento de vulnerabilidades en la red.	Sí
	Administración de parches para macOS	Si
	Poseer capacidad para inventariar dispositivos (windows, linux y Mac)	Sí
	Protección de vulnerabilidades en tiempo real	Sí
	Implementar medidas de protección contra exploits conocidos	Sí
	Información en la plataforma sobre cada CVE	Sí
	Actualización en tiempo real de vulnerabilidades	Sí
	Cubrir al menos 160,000 vulnerabilidades heredadas, igual o superior a las presentadas en el NIST	Sí
	Poseer definiciones de sistemas operativos	Sí

	Permitir la ejecución de comandos en todos los puntos de la red que tengan agentes	Sí
	Librería de scripts públicos con más de 250 scripts	Sí
	Librería de scripts públicos de múltiples fuentes	Sí
	Deberá poder permitir la visibilidad del porcentaje de cumplimiento de compliance según benchmark del NIST mínimamente de sistemas operativos windows y linux	Si
AGENTE		
	Los agentes deben poder escanear al menos la plataforma Windows, Linux y Mac.	Si
	Los agentes deben poder parchear al menos la plataforma Windows, Linux y Mac.	Si
	El agente debe poder parchearse a sí mismo.	Si
INTEGRACIONES Y REPORTEES		
	La plataforma debe soportar integraciones con SIEMs (Splunk, Sumo Logic y más).	Si
	La plataforma debe soportar integraciones con cualquier software via API.	Si
	Debe soportar integraciones vía SAML2 con los sistemas más conocidos (ej.: Okta, Ping Identity y más).	Si
	La plataforma debe poder soportar la integración con herramientas de gestión de incidentes, para la gestión, seguimiento y análisis forense de incidentes de seguridad de forma automatizada.	Si
	La plataforma debe poder generar informes sobre vulnerabilidades encontradas en uno de los siguientes tipos: formatos PDF con exportación a CSV, PDF Debe de poder generar reportes ejecutivos y técnicos. • Resumen ejecutivo, con información resumida. • Informe detallado, con toda la información técnica necesaria para que los lectores reproduzcan los problemas identificados.	Si

	Debe tener un tablero con resultados en tiempo real de las vulnerabilidades existentes.	Si
	Informe de riesgo integrado en la misma plataforma.	Si
	Soporte de informes de riesgos de múltiples aplicaciones.	Si
	Debe contar con una herramienta de reportería externa que permita realizar gráficos sobre las remediaciones para medir diferentes KPIs.	Si
	Debe contar con un dashboard de nivel de cumplimiento de compliance de los equipos gestionados.	Si
	La plataforma debe poder gestionar inventarios de dispositivos.	Si
Carta de autorización del Fabricante		
	Carta de Autorización del Fabricante	Si
Soporte técnico - Requisitos de Formación Técnica del Personal del Oferente		
	Para garantizar una correcta instalación, configuración y operación de los sistemas ofertados, el oferente deberá acreditar que al menos uno de los profesionales técnicos asignados al proyecto cuenta con certificaciones emitidas por instituciones de formación reconocidas en el país de origen del fabricante de la solución propuesta, las cuales no necesariamente deben ser emitidas por el fabricante, pero sí deben provenir de entidades reconocidas oficialmente en dicho país, asegurando que el personal posea conocimientos alineados con las normativas, prácticas y estándares vigentes en el ecosistema tecnológico donde se diseñaron los productos; además, además deberá contar con profesionales técnicos al menos uno, con una certificación específica emitida por el fabricante de la solución propuesta o una entidad autorizada por este, validando su competencia en la instalación, configuración y operación de la solución, presentando ambos requisitos mediante certificados escaneados acompañados de los currículum de los profesionales técnicos propuestos como parte de la documentación de la oferta.	Si

ITEM 2 - Implementación de Solución de Seguridad y Gestión de Eventos para 1000 activos

N°	Descripción del Requerimiento	Exigido
	Capacidad para identificar amenazas y anomalías en tiempo real mediante análisis avanzado de logs y correlación de eventos, utilizando reglas predefinidas y personalizables basadas en frameworks como MITRE ATT&CK, con soporte para detección de malware, rootkits y comportamientos anómalos mediante algoritmos de aprendizaje automático.	Si

	Ejecución automática de acciones correctivas ante incidentes detectados, como bloqueo de direcciones IP, aislamiento de endpoints, terminación de procesos maliciosos o ejecución de scripts personalizados, con registro detallado y auditable de todas las acciones para análisis post-incidente.	Si
	Capacidad para correlacionar datos de múltiples fuentes (endpoints, nube, firewalls, IDS/IPS) para identificar patrones de amenazas sofisticadas, como ataques persistentes avanzados (APTs) o movimiento lateral, con enriquecimiento de eventos mediante inteligencia de amenazas externa.	Si
	Generación de informes automatizados y auditorías detalladas para cumplir con regulaciones como PCI DSS, GDPR, HIPAA, ISO 27001 y NIST 800-53.	Si
	Integración con soluciones de seguridad, sistemas de ticketing y plataformas de comunicación (como ejemplo Slack, ServiceNow, Jira) mediante APIs bidireccionales y webhooks, permitiendo intercambio de datos en tiempo real y sincronización de alertas y acciones.	Si
	Creación de flujos de trabajo personalizados para reducir la intervención manual en la gestión de incidentes, con soporte para lógica condicional, priorización de alertas y automatización de tareas repetitivas, adaptándose al contexto específico de cada incidente.	Si
	Capacidad para manejar grandes volúmenes de datos en entornos complejos (nube, híbridos, red local) mediante arquitecturas escalables con clústeres, balanceo de carga y alta disponibilidad, asegurando procesamiento eficiente de eventos por segundo (EPS).	Si
	Interfaz intuitiva con dashboards personalizables, visualización en tiempo real de eventos de seguridad y soporte para personalización de reglas, alertas y flujos de trabajo, incluyendo control de acceso basado en roles (RBAC) para usuarios técnicos y no técnicos.	Si
	Protección de infraestructuras críticas mediante un proxy inverso con tunelización Zero Trust, utilizando túneles cifrados basados para exponer recursos privados sin abrir puertos, con autenticación centralizada, control de acceso basado en roles y políticas de confianza, soporte para balanceo de carga, certificados SSL automáticos y compatibilidad con entornos distribuidos detrás de firewalls restrictivos o CGNAT.	Si
	Capacidad para realizar búsqueda proactiva de amenazas (threat hunting) mediante consultas avanzadas en datos históricos, reconstrucción de líneas temporales de incidentes y correlación retrospectiva para identificar amenazas persistentes no detectadas inicialmente.	Si
	Soporte para colaboración en equipos de respuesta a incidentes, con gestión centralizada de alertas, asignación de roles, notificaciones en tiempo real y herramientas integradas de comunicación para coordinar acciones entre analistas y equipos externos.	Si

	Adaptabilidad a entornos de baja conectividad o recursos limitados, mediante agentes ligeros, análisis offline y flujos de trabajo optimizados, garantizando operatividad en escenarios remotos, industriales o con infraestructura restringida.	Si
	Soporte para análisis forense digital, incluyendo recolección automatizada de evidencia y generación de informes forenses detallados para investigaciones legales o auditorías.	Si
	Capacidad para detectar y responder a amenazas en entornos multi-nube, integrando APIs nativas de plataformas como AWS, Azure y GCP, con monitoreo de configuraciones de seguridad y detección de accesos no autorizados.	Si
	Implementación de políticas de seguridad basadas en el principio de confianza cero (Zero Trust), verificando continuamente identidades, dispositivos y conexiones para prevenir accesos no autorizados en redes híbridas.	Si
	Automatización de la gestión de vulnerabilidades, incluyendo escaneo continuo de activos, priorización de riesgos basada en criticidad y correlación con exploits conocidos para mitigar amenazas proactivamente.	Si
	Capacidad para monitorear el comportamiento de usuarios y entidades para detectar actividades sospechosas, como accesos anómalos o exfiltración de datos, mediante análisis de patrones y desviaciones.	Si
	Soporte para integración con sistemas de inteligencia de amenazas de código abierto y comerciales, permitiendo enriquecimiento automático de alertas con datos contextuales sobre actores de amenazas, IOCs y TTPs.	Si
	Generación de métricas y KPIs de seguridad en tiempo real, con dashboards que muestren tendencias de incidentes, tiempos de respuesta y efectividad de controles, facilitando la toma de decisiones estratégicas.	Si
	Capacidad para implementar y gestionar playbooks de respuesta a incidentes, con plantillas predefinidas y personalizables para estandarizar procesos de mitigación y recuperación ante ciberataques.	Si
	Soporte para entornos de red definidos por software (SDN) y contenedores (Docker, Kubernetes), con monitoreo de tráfico, detección de anomalías y respuesta automatizada en arquitecturas modernas.	Si
	Soporte para anonimizar datos sensibles en logs y reportes para cumplir con regulaciones de privacidad, garantizando que la información personal no sea expuesta durante análisis o auditorías.	Si

	Capacidad para gestionar incidentes en entornos IoT, con monitoreo de dispositivos conectados, detección de comportamientos anómalos y segmentación de red para limitar el impacto de compromisos.	Si
	Soporte para la gestión de activos de TI y OT, con inventarios dinámicos, categorización por criticidad y correlación con eventos de seguridad para priorizar respuestas a incidentes.	Si
	Capacidad para integrarse con sistemas de backup y recuperación ante desastres, automatizando la restauración de sistemas comprometidos y verificando la integridad de datos restaurados.	Si
	Soporte para capacitación y simulaciones de phishing, con integración de resultados en flujos de monitoreo para identificar usuarios de alto riesgo y reforzar la concienciación en seguridad.	Si
	Capacidad para detectar y mitigar ataques de denegación de servicio (DDoS) mediante análisis de tráfico, bloqueo dinámico de fuentes maliciosas y notificaciones a proveedores de red.	Si

ITEM 3 - Diseño e implementación de Centro de Operaciones de Seguridad por 2 años.

N°	Descripción del Requerimiento	Exigido
Evaluación y Planificación Inicial		
	Identificar y documentar los requisitos específicos de seguridad de la organización, alineando los objetivos del SOC con las metas estratégicas y necesidades operativas.	Si
	Realizar un análisis de riesgos exhaustivo para identificar vulnerabilidades, amenazas y su impacto potencial, priorizando activos críticos y considerando normativas aplicables.	Si

	Desarrollar, implementar y documentar políticas de Seguridad de la Información conforme a ISO/IEC 27001:2022, incluyendo al menos: - Seguridad de la Información - Control de Acceso - Gestión de Activos - Gestión de Incidentes - Gestión de Riesgos - Uso Aceptable de Activos - Protección de Datos y Privacidad - Seguridad Física y Ambiental - Gestión de Proveedores - Concienciación y Formación - Copias de Seguridad - Gestión de Cambios	Si
	Establecer un proceso automatizado de gestión de parches para sistemas, aplicaciones y dispositivos de red, asegurando remediación oportuna de vulnerabilidades críticas.	Si
	Elaborar un plan detallado de implementación del SOC, incluyendo cronogramas, asignación de recursos, roles, responsabilidades y un presupuesto estimado.	Si
	Definir un modelo de madurez del SOC basado en frameworks como CIS Controls, NIST Cybersecurity Framework (CSF), CMMI o SIM3, para evaluar el progreso de las capacidades operativas, técnicas y de gobernanza, y establecer metas de mejora continua.	Si
	Realizar un inventario completo de activos de TI (hardware, software, datos) para determinar el alcance del monitoreo y protección del SOC.	Si
	Establecer una recomendación de plan de continuidad del negocio y recuperación ante desastres (BCDR) específico para las operaciones del SOC, incluyendo redundancia de sistemas críticos.	Si
Diseño de la Arquitectura		
	Diseñar una arquitectura de red y sistemas robusta para el SOC, definiendo configuraciones seguras de hardware, software y segmentación de red.	Si
	Seleccionar tecnologías de seguridad (SIEM, IDS/IPS, herramientas forenses, EDR), priorizando soluciones interoperables, escalables y sostenibles, incluyendo opciones open source.	Si

	Definir procesos operativos estándar (SOP) para monitoreo, detección, respuesta y escalamiento de incidentes, asegurando claridad y adaptabilidad.	Si
	Diseñar un modelo de integración de threat intelligence para enriquecer la detección y respuesta a amenazas, utilizando feeds externos e internos.	Si
	Establecer una arquitectura de almacenamiento y gestión de logs que garantice alta disponibilidad, retención conforme a normativas y capacidad para manejar picos de datos.	Si
	Definir requisitos de seguridad física para las instalaciones del SOC, incluyendo control de acceso, videovigilancia y protección contra desastres naturales.	Si
Implementación Técnica		
	Gestionar una herramienta para relevamiento de estado de compliance, alineados con las mejores prácticas de ciberseguridad.	Si
	Integrar herramientas de seguridad (SIEM, IDS, SOAR, EDR) con la infraestructura existente, desplegando sensores y agentes en puntos críticos de la red.	Si
	Configuración segura de servidores (hardening) para minimizar vulnerabilidades, siguiendo guías reconocidas de buenas prácticas.	Si
	Realizar pruebas de aceptación (UAT) para validar la funcionalidad, interoperabilidad y rendimiento de las herramientas y sistemas implementados.	Si
	Configurar un sistema de respaldo y restauración para los datos y configuraciones del SOC, garantizando la continuidad operativa.	Si
	Implementar controles de acceso basados en el principio de privilegio mínimo para todos los sistemas y herramientas del SOC.	Si
Desarrollo de Capacidades Operacionales		
	El proveedor deberá reclutar y capacitar un equipo de profesionales, incluyendo al menos un Analista de Centro de Operaciones de Seguridad (SOC Analyst) de nivel inicial y de Tecnologías de la Información (TI), asegurando que cuenten con las competencias técnicas y operativas necesarias para cumplir con los objetivos del proyecto en la instalaciones de la convocante.	Si
	Desarrollar guías operativas, manuales y playbooks para la gestión del SOC, complementados con simulacros y pruebas de procedimientos.	Si

	Implementar un sistema de monitoreo continuo 24x7 para eventos y alertas de seguridad, con priorización de amenazas y correlación de eventos.	Si
	Establecer procedimientos para análisis rápido y respuesta efectiva a incidentes, incluyendo playbooks.	Si
	Revisar y actualizar regularmente herramientas, procesos y procedimientos del SOC para adaptarse a nuevas amenazas, tecnologías y lecciones aprendidas.	Si
	Proveer un servicio SOC 8x5 en ubicación designada, con personal de la institución supervisado por un analista de la contratante, servicio de monitoreo remoto 24x7 para horarios nocturnos y fuera de oficina.	Si
	Implementar un servicio SIEM que permita incorporar nuevos dispositivos sin costos adicionales de licenciamiento ni renovaciones posteriores al contrato. Según capacidades disponibles del hardware proveído por la contratante.	Si
	El proveedor deberá implementar una herramienta SOAR interoperable con todos los componentes del Centro de Operaciones de Seguridad (SOC), diseñada para optimizar la colaboración entre analistas y automatizar procesos de respuesta a incidentes de seguridad. La solución debe cumplir con los siguientes requisitos: • Integración seamless con los sistemas existentes del SOC, incluyendo SIEM, firewalls, IDS/IPS, y herramientas de análisis de amenazas, mediante APIs estándares o conectores preconfigurados. • Compatibilidad con plataformas de gestión de incidentes y herramientas de colaboración utilizadas por los analistas. • Capacidad para automatizar el análisis y descarte de falsos positivos mediante consultas en tiempo real a fuentes de IOC confiables, como bases de datos de amenazas públicas o suscripciones privadas de inteligencia de amenazas. El Proveedor deberá cubrir los costos de ser necesario. • Funcionalidad para identificar IPs sospechosas y agregarlas automáticamente a una lista negra en dispositivos de seguridad según reglas predefinidas y umbrales configurables. • Automatización de flujos de trabajo para reducir el tiempo de respuesta (MTTR - Mean Time to Resolve)	Si
	Establecer un programa de threat hunting proactivo para identificar amenazas avanzadas no detectadas por sistemas automatizados.	Si
	Implementar un plan de capacitación continua para el personal del SOC, incluyendo certificaciones, simulacros avanzados y participación en ejercicios de ciberseguridad.	Si
	Configurar un sistema de gestión de incidentes para documentar, rastrear y analizar incidentes de seguridad, asegurando trazabilidad y auditoría.	Si
Gestión de Cumplimiento y Reportes		

	Generar informes mensuales sobre el estado de seguridad, incidentes y métricas de desempeño del SOC, adaptados a la alta dirección y equipos técnicos.	Si
	Cumplir con métricas de desempeño alineadas con estándares internacionales como NIST SP 800-61, ISO/IEC 27001, e ISO/IEC 27035: - Tiempo medio de detección (MTTD) < 30 minutos - Tiempo medio de respuesta (MTTR) crítico < 2 horas - Falsos positivos < 10% - Inactividad no planificada < 0.1% - Vulnerabilidades críticas remediadas > 80% dentro de SLA - Amenazas identificadas proactivamente > 2/mes - Tasa de contención de incidentes > 90%	Si
	Realizar auditorías internas anual del SOC para verificar el cumplimiento de políticas, normativas y estándares (ej. ISO 27001, GDPR).	Si
	Establecer un proceso de gestión de evidencias forenses para investigaciones de incidentes, asegurando la cadena de custodia y cumplimiento legal.	Si
	Implementar un sistema de retroalimentación para mejorar procesos del SOC, basado en lecciones aprendidas de incidentes y simulacros.	Si
Alcance Detallado		
	Monitorear aproximadamente 700 endpoints, con capacidad para escalar a futuros activos.	Si
	Procesar un volumen de datos/logs de aproximadamente 5 GB/día, con infraestructura preparada para incrementos.	Si
	Incluir en el alcance la protección de entornos híbridos (on-premise, nube, dispositivos móviles), asegurando visibilidad completa.	Si
	Definir un SLA claro para la incorporación de nuevos activos al monitoreo del SOC, sin impacto en el rendimiento.	Si
Gestión de Terceros y Colaboración Externa		
	Definir un protocolo de comunicación y colaboración con entidades externas, como CERTs, ISACs o fuerzas del orden, para la gestión de incidentes críticos.	Si

	Implementar un proceso de evaluación y monitoreo de terceros que interactúen con el SOC, asegurando cumplimiento de seguridad.	Si
Pruebas de Penetración Semestrales		
	Ejecución de pruebas éticas de penetración (externas e internas) siguiendo estándares reconocidos como OWASP, NIST SP 800-115, o PTES. Las pruebas incluirán simulación de ataques reales	Si
	Reconocimiento: Recopilación de información sobre la infraestructura objetivo.	Si
	Escaneo de Vulnerabilidades: Identificación de posibles vulnerabilidades mediante herramientas automatizadas y manuales.	Si
	Explotación: Intento de explotación de las vulnerabilidades identificadas para determinar el nivel de riesgo.	Si
	Post-Explotación: Análisis del impacto de las vulnerabilidades explotadas y extracción de datos sensibles si es posible.	Si
	Evaluación de Segmentos Específicos Aproximadamente 700 dispositivos entre servidores físicos y máquinas virtuales. Segmento de Usuarios: Pruebas de seguridad en estaciones de trabajo y dispositivos de los usuarios. Wi-Fi: Evaluación de la seguridad de las redes inalámbricas.	Si
	Después de implementar las recomendaciones iniciales, se realizará un re-testing para verificar la efectividad de las acciones correctivas.	Si
	Entrega de un informe detallado con vulnerabilidades identificadas, nivel de riesgo (bajo, medio, alto, crítico), y recomendaciones de mitigación. El informe incluirá un plan de remediación priorizado.	Si
	Plan de Acciones priorizado: Recomendaciones para mitigar las vulnerabilidades encontradas, categorizadas por criticidad, urgencia y relevancia.	Si
	Remediaciones: Las remediaciones se hacen en concordancia con el personal de TI del SNPP. La empresa adjudicada debe brindar el acompañamiento necesario.	Si
	Horas mínimas requeridas para pentesting, reportes y asistencia: 2080 horas.	Si

Indicadores de cumplimiento:		
	Informe de pruebas de penetración entregado dentro de los 30 días hábiles posteriores a la finalización de las pruebas.	Si
	Mitigación de vulnerabilidades críticas y altas dentro de los 90 días corridos establecidos, que no requieran inversión económica.	Si
	Evidencia de pruebas de verificación post-remediación para confirmar la resolución de vulnerabilidades	Si
	Se priorizará la contratación de empresas locales especializadas en ciberseguridad para realizar las pruebas, promoviendo el desarrollo de capacidades técnicas nacionales y la sostenibilidad económica	Si

ÍTEM 4 - Diseño e Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI-TI)

N°	Descripción del Requerimiento	
Evaluación y Planificación Inicial		
	Realizar un análisis detallado de la situación actual de la seguridad de la información en la organización, incluyendo la identificación y clasificación de activos, procesos y sistemas críticos. Utilizar frameworks como NIST CSF o COBIT para estructurar el análisis, priorizando activos según su criticidad (confidencialidad, integridad, disponibilidad)., documentando riesgos asociados a datos sensibles del sector educativo.	Si
	Determinar el alcance y las áreas involucradas en el establecimientos del SGSI-TI	Si
	Implementar un inventario automatizado de activos con herramientas de inventario de activos.	Si
	Determinar los requisitos de seguridad de la información basados en las necesidades de la organización, normativas aplicables y estándares internacionales como ISO/IEC 27001:2022.	Si
	Realizar un análisis de nivel de cumplimiento documental frente a la ISO 27001 y definir un plan de acción priorizado para cerrar brechas identificadas.	Si
2. Diseño e Implementación del SGSI		

	Seleccionar e implementar controles y medidas de seguridad adecuados (Anexo A de ISO 27001) para proteger la información y los activos críticos.	Si
	Priorizar controles técnicos y organizativos para mitigar riesgos de alto impacto en el sector educativo, como accesos no autorizados a datos sensibles.	Si
	Crear políticas, procedimientos y documentación necesaria para el funcionamiento del SGSI, estandarizando documentos con plantillas basadas en ISO 27001. Incluir políticas específicas como gestión de accesos, manejo de incidentes y protección de datos personales, manteniendo un repositorio centralizado y accesible en plataformas de gestión documental.	Si
	Capacitar al personal en prácticas de seguridad de la información y concienciación sobre su importancia, diseñando un programa de formación continua con simulaciones de phishing y talleres interactivos y evaluar el impacto mediante encuestas y pruebas post-formación.	Si
	Implementar procesos operativos para la gestión continua de la seguridad de la información, estableciendo un ciclo PDCA (Planificar, Hacer, Verificar, Actuar). Automatizar procesos como la gestión de parches y actualizaciones de seguridad, y designar responsables claros para cada proceso operativo.	Si
3. Operación del SGSI		
	Establecer mecanismos para la monitorización continua de la seguridad y la detección de incidentes, implementando un sistema SIEM con alertas en tiempo real. Configurar tableros de control para visualizar métricas de seguridad e integrar inteligencia de amenazas para identificar amenazas emergentes.	Si
	Desarrollar procedimientos para la respuesta efectiva a incidentes de seguridad y la recuperación de operaciones, basados en NIST 800-61. Realizar simulacros semestrales de incidentes y establecer acuerdos de nivel de servicio (SLA) para tiempos de respuesta y recuperación.	Si
	Realizar auditorías internas periódicas para evaluar la conformidad del SGSI con las políticas y procedimientos establecidos, programando auditorías anuales para acelerar la madurez del SGSI. Capacitar auditores internos en ISO 27001 y usar herramientas de gestión de auditorías para optimizar el proceso.	Si
	Revisar regularmente el desempeño del SGSI por parte de la alta dirección para asegurar su eficacia y adecuación, mediante reuniones trimestrales con presentación de informes ejecutivos que incluyan KPIs de seguridad y recomendaciones estratégicas, alineadas con los objetivos del SNPP.	Si
	Realizar una auditoría interna al año de implementado para verificar la conformidad, con auditores certificados en ISO 27001.	Si

4. Programa de Capacitación Gamificado para Usuarios de TI		
	Se implementará un programa de capacitación gamificado, liderado por el líder de proyecto, dirigido a usuarios de TI para garantizar el cumplimiento de políticas de seguridad. Incluirá ejemplos prácticos de amenazas comunes en el sector educativo, como phishing, ransomware y explotación de vulnerabilidades en sistemas.	Si
	Implementar programas de formación para empleados en todos los niveles, cubriendo concienciación sobre ciberseguridad, divididos en módulos cortos (1-2 horas) para facilitar la asistencia. Ofrecer sesiones presenciales y en línea.	Si
	Suscribir a cursos especializados en español para 10 funcionarios que incluyan Marco MITRE ATT&CK, análisis de vulnerabilidades, monitorización con sistemas de gestión de eventos de seguridad y ataques contra entornos Microsoft. Priorizar cursos con laboratorios prácticos, actualizados con las últimas tácticas de MITRE ATT&CK, con acceso durante la duración del contrato y formación 100% online. Marco MITRE ATT&CK: Análisis de tácticas, técnicas y procedimientos (TTP) de adversarios, con laboratorios prácticos actualizados a las últimas versiones del marco (2025). Análisis de Vulnerabilidades: Metodologías para identificar, evaluar y mitigar vulnerabilidades, con enfoque en entornos Microsoft. Monitorización con Sistemas de Gestión de Eventos de Seguridad: Uso de herramientas como ELK (Elasticsearch, Logstash, Kibana) y Wazuh para detección proactiva de amenazas. Ataques contra Entornos Microsoft: Técnicas ofensivas y defensivas para entornos Microsoft, incluyendo abuso de tokens, explotación de permisos y ataques a Active Directory.	Si
	Contenido disponible en la plataforma en línea durante la vigencia del contrato, con soporte personalizado 1 a 1 (telefónico, e-mail, Teams, etc.).	Si
Plataforma de Formación		
	Los cursos se impartirán a través de una plataforma en línea, accesible 24/7, con grabaciones, material de apoyo, ejercicios resueltos y contenido complementario.	Si
	Soporte 1 a 1 con instructores expertos, disponible mediante: • Teléfono. • Correo electrónico. • Microsoft Teams u otras plataformas acordadas.	Si
	Tiempo de respuesta: Máximo 24 horas hábiles para consultas por e-mail; soporte telefónico en horario laboral (a definir con el cliente).	Si

	Evaluaciones prácticas obligatorias al finalizar cada módulo o curso, con un umbral de aprobación del 70%.	Si
5. Auditorías y Evaluaciones Continuas		
	Realizar auditorías anuales del SGSI y análisis de brechas para verificar conformidad con ISO/IEC 27001:2022 y detectar vulnerabilidades, coordinando con el calendario de TI para minimizar interrupciones. Combinar auditorías internas y externas, usando herramientas de análisis de vulnerabilidades para análisis de brechas automatizados, con énfasis en la protección de datos sensibles del sector educativo.	Si
	Desarrollar un plan de auditoría que cubra los 14 dominios de ISO 27001, priorizando dominios críticos como gestión de accesos y respuesta a incidentes. Incluir pruebas específicas para datos sensibles (p.ej., DPI, historias clínicas) y documentar el plan en un formato claro y auditable.	Si
	Ejecutar auditorías mediante entrevistas, revisión documental y análisis de procesos, capacitando al equipo auditor en técnicas de entrevistas efectivas. Usar listas de verificación basadas en ISO 27001 para estandarizar la revisión e involucrar a todas las áreas relevantes (TI, legal, operaciones).	Si
	Generar un informe detallado con hallazgos, no conformidades, riesgos identificados y recomendaciones específicas, estructurado con un resumen ejecutivo para la alta dirección. Clasificar hallazgos por prioridad (crítico, alto, medio, bajo) e incluir un plan de acción con plazos y responsables.	Si
	Implementar un plan de acción para corregir no conformidades y mitigar riesgos, con plazos definidos y responsables asignados, usando herramientas de gestión de proyectos para seguimiento. Establecer revisiones mensuales para monitorear el progreso y asignar recursos específicos para acciones críticas.	Si
6. Indicadores de Cumplimiento (Auditorías)		
	Presentar el informe de auditoría dentro de los 15 días hábiles posteriores a la finalización, automatizando la generación con plantillas predefinidas.	Si
	Implementar al menos el 80% de las acciones correctivas dentro de los plazos establecidos 90 días. Identificar cuellos de botella y escalar problemas críticos a la alta dirección si es necesario.	Si

DETALLES DE LOS SERVICIOS SOLICITADOS PARA COTIZACIÓN

Para facilitar la elaboración de una cotización precisa, se detallan los servicios requeridos, agrupados en categorías clave. Los proveedores deberán incluir un desglose de costos, cronograma de ejecución y especificaciones técnicas para cada ítem.

1. Infraestructura

- **Servidores o Virtualización:**
 - El hardware será proveído por la convocante.

- Configuración para soportar (SIEM) el sistema de ticket y orquestador de seguridad.
- Instalación y pruebas en las instalaciones de la organización.
- **Almacenamiento Seguro:**
 - El proveedor deberá realizar las configuraciones necesarias para garantizar la rotación y el backup de la información.
 - Configuración de backups automatizados.
- **Redes:**
 - Implementación de herramientas de monitoreo continuo y remediación en 1000+ endpoints.
- **Entregables:**
 - Informe de instalación y configuración.
 - Pruebas de rendimiento y escalabilidad.

2. Consultoría para SGSI y SOC

- **Diagnóstico Inicial:**
 - Auditorías CIS y OWASP Top 10 en 50 activos críticos (Infra SNPP).
 - Escaneo de vulnerabilidades con OpenVAS en redes y endpoints.
 - Entrevistas a stakeholders clave.
 - Informe técnico con matriz de riesgos y línea base (MTTD, MTTR, incidentes).
- **Diseño e Implementación del SGSI:**
 - Desarrollo de 10 políticas y 30 controles prioritarios (ISO 27001, NIST CSF, CIS Controls).
 - Recomendación de hardening según benchmarks NIST.
- **Implementación del SOC:**
 - Instalación y configuración de (SIEM).
 - Integración de Ticket para gestión de incidentes y SOAR para orquestación.
 - Protocolo de coordinación entre SOC presencial (8x5) y remoto (7x24).
- **Creación del CSIRT:**
 - Definición de 3 roles (coordinador, analista, forense).
 - Desarrollo de playbooks para phishing, ransomware y DDoS.
 - Simulaciones de incidentes (3 escenarios: phishing, ransomware, DDoS).
- **Auditorías y Optimización:**
 - Auditorías semestrales (Meses 12, 18, 24) para verificar cumplimiento.
 - Optimización de reglas de detección y reducción de falsos positivos (50% en Mes 4).
 - Informes semestrales con métricas (MTTD $\leq$ 60 min, MTTR reducido en 70%).
- **Entregables:**
 - Políticas SGSI (10 documentos).
 - Dashboards SOC (5 vistas en Wazuh).
 - Playbooks operativos (3 escenarios).
 - Informes de auditoría (inicial y semestrales).
 - Matriz de riesgos actualizada.

3. Capacitación

- **Formación Técnica (300 horas, 2 técnicos):**
 - 10 meses, 30 horas/mes, formato presencial/híbrido.
 - Temario:
 - Marco de trabajo Mitre
 - Especialista en análisis de vulnerabilidades
 - Monitorización con Wazuh
 - 10 ataques Contra entornos microsoft
 - Entregables: Certificados, manuales de capacitación.
- **Sensibilización (15 horas, 700 colaboradores):**
 - 5 sesiones grupales de 3 horas (140 personas por sesión, formato híbrido).
 - Contenido gamificado: simulaciones de phishing, cuestionarios interactivos.
 - Entregables: Material educativo, informe de participación (80% de cobertura en Mes 3).

4. Operación del SOC

- **Monitoreo y Respuesta:**
 - Operación 8x5 presencial (1 analista dedicado en sitio).
 - Operación 7x24 remota (equipo del proveedor).
 - Monitoreo de 1000+ endpoints con Wazuh.
 - Resolución de incidentes críticos en $\leq$ 24 horas (100% en Mes 7).
- **Mantenimiento:**

- Actualización de reglas y playbooks (anual).
- Gestión de infraestructura (servidores, almacenamiento, redes).
- Soporte técnico por 24 meses.
- **Entregables:**
 - Informes mensuales de métricas (MTTD, MTTR, incidentes).
 - Registro de incidentes resueltos.

5. Soporte Post-Implementación

- **Asistencia Técnica:**
 - 3 meses de soporte remoto (Meses 11-13).
 - Resolución de consultas técnicas y ajustes operativos.
- **Transferencia de Conocimiento:**
 - 5 sesiones prácticas (Meses 8-10) para operar Wazuh, osTicket, y TheHive.
 - Entrega de 50 documentos técnicos en español.
 - Simulación final de incidente (Mes 24) para validar autonomía.
- **Entregables:**
 - Manual de operación del SOC.
 - Guía de mantenimiento de herramientas.
 - Acta de transferencia firmada.

6. Garantía

- Garantía de 24 meses para software (Wazuh, osTicket, TheHive, OpenVAS).
- Soporte para corrección de errores y actualizaciones críticas.
- Entregables: Contrato de garantía, SLA (Service Level Agreement).

ENTREGABLES

- Políticas SGSI (mínimo 10 documentos, alineados con ISO 27001).
- Dashboards SOC (mínimo 5 vistas en Wazuh).
- Playbooks operativos para phishing, ransomware y DDoS.
- Informes de auditoría (inicial, semestrales).
- Matriz de riesgos y plan de mitigación.
- Documentación técnica (50 documentos en español).
- Roadmap para 12 meses post-proyecto.
- Plan de transferencia de conocimiento

De las MIPYMES

En procedimientos de Menor Cuantía, la aplicación de la preferencia reservada a las MIPYMES prevista en el artículo 34 inc b) de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas" será de conformidad con las disposiciones que se emitan para el efecto. Son consideradas Mipymes las unidades económicas que, según la dimensión en que organicen el trabajo y el capital, se encuentren dentro de las categorías establecidas en el Artículo 4° de la Ley N° 7444/25 QUE MODIFICA LA LEY N° 4457/2012 "PARA LAS MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS", y se ocupen del trabajo artesanal, industrial, agroindustrial, agropecuario, forestal, comercial o de servicio.

Plan de entrega de los bienes

La entrega de los bienes se realizará de acuerdo al plan de entrega, indicado en el presente apartado. El proveedor se encuentra facultado a documentarse sobre cada entrega. Así mismo, de los documentos de embarque y otros que deberá suministrar el proveedor indicado a continuación:

La prestación de los servicios se realizará de acuerdo con el plan de prestación, indicados en el presente apartado. Así mismo, de los documentos de embarque y otros que deberá suministrar el proveedor indicados a continuación:

ÍTEM 1 - Suscripción de software identificación de vulnerabilidades y remediación para 600 activos con soporte remoto por 24 meses.

Una vez emitida la orden de servicio y recepcionada por el oferente adjudicado, en un plazo máximo de 7 (siete) días corridos para la entrega de adjudicación de licencias o suscripción correspondientes.

ÍTEM 2 - Implementación SOC

Una vez emitida la orden de servicio y recepcionada por el oferente adjudicado, en un plazo máximo de 90 (noventa) días corridos para la implementación y puesta en marcha. **ÍTEM 3** - Diseño e Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI)

Una vez emitida la orden de servicio y recepcionada por el oferente adjudicado, en un plazo máximo de 90 (noventa) días corridos para la implementación y puesta en marcha.

ÍTEM 4 Pentesting. Una vez emitida la orden de servicio y recepcionada por el oferente adjudicado, en un plazo máximo de 60 (sesenta) días corridos para el servicio.

Plan de prestación de los servicios

La prestación de los servicios se realizará de acuerdo al plan de prestación, indicados en el presente apartado. El proveedor se encuentra facultado a documentarse sobre cada prestación.

No Aplica

Planos y diseños

Para la presente contratación se pone a disposición los siguientes planos o diseños:

No Aplica

Embalajes y documentos

El embalaje, la identificación y la documentación dentro y fuera de los paquetes serán como se indican a continuación:

No Aplica

Inspecciones y pruebas

Las inspecciones y pruebas serán como se indica a continuación:

No Aplica

CONDICIONES CONTRACTUALES

Esta sección constituye las condiciones contractuales a ser adoptadas por las partes para la ejecución del contrato.

Interpretación

1. Si el contexto así lo requiere, el singular significa el plural y viceversa; y "día" significa día corrido, salvo que se haya indicado expresamente que se trata de días hábiles.
2. Condiciones prohibidas, inválidas o inejecutables. Si cualquier provisión o condición del contrato es prohibida o resultase inválida o inejecutable, dicha prohibición, invalidez o falta de ejecución no afectará la validez o el cumplimiento de las otras provisiones o condiciones del contrato.

Documentación electrónica

Cuando las documentaciones se expidan de manera electrónica en cumplimiento de la Ley N° 6715 "DE PROCEDIMIENTOS ADMINISTRATIVOS" y la Ley N° 6822 "DE SERVICIOS DE CONFIANZAS PARA LAS TRANSACCIONES ELECTRÓNICAS, DEL DOCUMENTO ELECTRÓNICO Y LOS DOCUMENTOS TRANSMISIBLES ELECTRÓNICOS, las mismas se considerarán válidas a los efectos de dar cumplimiento a los requerimientos y obligaciones contractuales, salvo que las normativas exijan una forma determinada.

Formalización de la contratación

Se formalizará esta contratación mediante:

Contrato

Documentación requerida para la firma del contrato

Luego de la notificación de adjudicación, el proveedor deberá presentar en el plazo establecido en las reglamentaciones vigentes, los documentos indicados en el presente apartado.

1. Personas Físicas / Jurídicas

- Certificado de no encontrarse en quiebra o en convocatoria de acreedores expedido por la Dirección General de Registros Públicos;

- Certificado de no hallarse en interdicción judicial expedido por la Dirección General de Registros Públicos;
- Constancia de no adeudar aporte obrero patronal expedida por el Instituto de Previsión Social.
- Certificado laboral vigente expedido por la Dirección de Obrero Patronal dependiente del Viceministerio de Trabajo, siempre que el sujeto esté obligado a contar con el mismo, de conformidad a la reglamentación pertinente - CPS
- En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para asumir todas las obligaciones emergentes del contrato hasta su terminación, el cual deberá estar inscripto en el registro de poderes.
- Certificado de cumplimiento tributario vigente a la firma del contrato.
- Declaración jurada en el que se manifieste que las condiciones verificadas por el Comité respecto a los supuestos del Art. 21 de la Ley N° 7021/22, se mantienen vigentes a la firma del contrato.

2. Documentos. Consorcios

- Cada integrante del Consorcio que sea una persona física o jurídica deberá presentar los documentos requeridos para oferentes individuales especificados en los apartados precedentes.
- Original o fotocopia de la Escritura Pública de constitución del Consorcio constituido
- Documentos que acrediten las facultades del firmante del contrato para comprometer solidariamente al consorcio.
- En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para asumir todas las obligaciones emergentes del contrato hasta su terminación.

La convocante deberá recurrir a fuentes oficiales para la verificación y comprobación del contenido declarado por el oferente que resultare adjudicado, con anterioridad a la firma del contrato. Si el oferente realizare una declaración jurada falsa, la adjudicación será revocada, la garantía de mantenimiento de oferta será ejecutada y los antecedentes serán remitidos a la Dirección Nacional de Contrataciones Públicas.

Indicadores de Cumplimiento de Contrato

El documento requerido para acreditar el cumplimiento contractual, será:

Planificación de indicadores de cumplimiento:

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA <i>(Se indica la fecha que debe presentar según el PBC)</i>
Cumplimiento contractual	Nota de Remisión	Contra entrega de los bienes recepcionados

Acta de
recepción
definitiva

Acta de
recepción
definitiva

ÍTEM 1 - Suscripción de software identificación de vulnerabilidades y remediación para 600 activos con soporte remoto por 24 meses.

Una vez emitida la orden de servicio y recepcionada por el oferente adjudicado, en un plazo máximo de 7 (siete) días corridos para la entrega de adjudicación de licencias o suscripción correspondientes.

ÍTEM 2 - Implementación SOC Una vez emitida la orden de servicio y recepcionada por el oferente adjudicado, en un plazo máximo de 90 (noventa) días corridos para la implementación y puesta en marcha.

ÍTEM 3 - Diseño e Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) Una vez emitida la orden de servicio y recepcionada por el oferente adjudicado, en un plazo máximo de 90 (noventa) días corridos para la implementación y puesta en marcha.

ÍTEM 4 Pentesting. Una vez emitida la orden de servicio y recepcionada por el oferente adjudicado, en un plazo máximo de 60 (sesenta) días corridos para el servicio.

De manera a establecer indicadores de cumplimiento, a través del sistema de seguimiento de contratos, la convocante deberá determinar el tipo de documento que acredite el efectivo cumplimiento de la ejecución del contrato, así como planificar la cantidad de indicadores que deberán ser presentados durante la ejecución. Por lo tanto, la convocante en este apartado y de acuerdo al tipo de contratación de que se trate, deberá indicar el documento a ser comunicado a través del módulo de Seguimiento de Contratos y la cantidad de los mismos.

Subcontratación

En caso de que aplique, la subcontratación del contrato deberá ser realizada conforme a las disposiciones contenidas en la Ley, el Decreto Reglamentario y la reglamentación que emita para el efecto la DNCP.

En caso de que la presentación del formulario de personas a subcontratar/subcontratadas, se realice en la etapa contractual, el Administrador del Contrato deberá evaluar el contenido del formulario a los efectos de constatar que el subcontratista no se encuentra comprendido en alguna de las causales de prohibición previstas en el Art. 21 de la Ley N° 7021/22, pudiendo requerir al proveedor o contratista, la información que sea necesaria.

Derechos Intelectuales

1. Los derechos de propiedad intelectual de todos los planos, documentos y otros materiales conteniendo datos e información proporcionada a la contratante por el proveedor, seguirán siendo, salvo prueba en contrario, de propiedad del proveedor. Si esta información fue suministrada a la contratante directamente o a través del proveedor por terceros, incluyendo proveedores de materiales, los derechos de propiedad intelectual de dichos materiales seguirán siendo de propiedad de dichos terceros.

2. Sujeto al cumplimiento por parte de la contratante del párrafo siguiente, el proveedor indemnizará y liberará de toda responsabilidad a la contratante, sus empleados y funcionarios en caso de pleitos, acciones o procedimientos administrativos, reclamaciones, demandas, pérdidas, daños, costos y gastos de cualquier naturaleza, incluyendo gastos y

honorarios por representación legal, que la contratante tenga que incurrir como resultado de la transgresión o supuesta transgresión de derechos de propiedad intelectual como patentes, dibujos y modelos industriales registrados, marcas registradas, derechos de autor u otro derecho de propiedad intelectual registrado o ya existente en la fecha del contrato debido a:

- a. La instalación de los bienes por el proveedor o el uso de los bienes en la República del Paraguay; y
- b. La venta de los productos producidos por los bienes en cualquier país.

Dicha indemnización no procederá si los bienes o una parte de ellos fuesen utilizados para fines no previstos en el contrato o para fines que no pudieran inferirse razonablemente del contrato. La indemnización tampoco cubrirá cualquier transgresión que resultará del uso de los bienes o parte de ellos, o de cualquier producto producido como resultado de asociación o combinación con otro equipo, planta o materiales no suministrados por el proveedor en virtud del contrato.

3. Si se entablara un proceso legal o una demanda contra la contratante como resultado de alguna de las situaciones indicadas en la cláusula anterior, la contratante notificará prontamente al proveedor y éste por su propia cuenta y en nombre de la contratante responderá a dicho proceso o demanda, y realizará las negociaciones necesarias para llegar a un acuerdo de dicho proceso o demanda.

4. Si el proveedor no notifica a la contratante dentro de treinta (30) días a partir del recibo de dicha comunicación de su intención de proceder con tales procesos o reclamos, la contratante tendrá derecho a emprender dichas acciones en su propio nombre.

5. La contratante se compromete, a solicitud del proveedor, a prestarle toda la asistencia posible para que el proveedor pueda contestar las citadas acciones legales o reclamaciones. La contratante será reembolsada por el proveedor por todos los gastos razonables en que hubiera incurrido.

6. La contratante deberá indemnizar y eximir de culpa al proveedor y a sus empleados, funcionarios y subcontratistas, por cualquier litigio, acción legal o procedimiento administrativo, reclamo, demanda, pérdida, daño, costo y gasto, de cualquier naturaleza, incluyendo honorarios y gastos de abogado, que pudieran afectar al proveedor como resultado de cualquier transgresión o supuesta transgresión de patentes, modelos de aparatos, diseños registrados, marcas registradas, derechos de autor, o cualquier otro derecho de propiedad intelectual registrado o ya existente a la fecha del contrato, que pudieran suscitarse con motivo de cualquier diseño, datos, planos, especificaciones, u otros documentos o materiales que hubieran sido suministrados o diseñados por la contratante o a nombre suyo.

Transporte

La responsabilidad por el transporte de los bienes será según se establece en los Incoterms.

Si no está de acuerdo con los Incoterms, la responsabilidad por el transporte deberá ser como sigue:

No Aplica

Confidencialidad de la información

Reserva de información en respuestas a aclaraciones.

En las respuestas a las solicitudes de aclaración, los oferentes deberán indicar si la información suministrada es de carácter reservado, debiendo precisar la norma legal que la establece como secreta o de carácter reservado, de conformidad a lo estipulado en la Ley N° 5282/14 "DE LIBRE ACCESO CIUDADANO A LA INFORMACIÓN PÚBLICA Y TRANSPARENCIA GUBERNAMENTAL"

Confidencialidad de la etapa de evaluación de ofertas.

No deberá darse a conocer información alguna acerca del análisis, aclaración y evaluación de las ofertas, mientras dure el mismo de conformidad con el artículo N° 52 de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas", ni sobre las recomendaciones relativas a la adjudicación, después de la apertura en público de las ofertas, a los oferentes ni a personas no involucradas en el proceso de evaluación, hasta que haya sido dictada la resolución de adjudicación cuando se trate de un solo sobre. Cuando se trate de dos sobres, la confidencialidad de la primera etapa será hasta la emisión del acto administrativo de selección de ofertas técnicas, reanudándose la confidencialidad después de la apertura en público de las ofertas económicas hasta la emisión de la resolución de adjudicación.

Confidencialidad en el procedimiento de contratación y el contrato.

La contratante y el proveedor deberán mantener confidencialidad y en ningún momento divulgarán a terceros, sin el consentimiento de la otra parte, documentos, datos u otra información que hubiera sido directa o indirectamente proporcionada por la otra parte en conexión con el contrato, antes, durante o después de la ejecución del mismo. No obstante, el proveedor podrá proporcionar a sus subcontratistas los documentos, datos e información recibidos de la contratante para que puedan cumplir con su trabajo en virtud del contrato. En tal caso, el proveedor obtendrá de dichos subcontratistas un compromiso de confidencialidad similar al requerido al proveedor en la presente cláusula.

La contratante no utilizará dichos documentos, datos u otra información recibida del proveedor para ningún uso que no esté relacionado con el contrato. Así mismo el proveedor no utilizará los documentos, datos u otra información recibida de la contratante para ningún otro propósito diferente al de la ejecución del contrato.

La obligación de las partes arriba mencionadas, no aplicará a la información que:

- 1) La contratante o el proveedor requieran compartir con otras instituciones que participan en el financiamiento del contrato,
- 2) Actualmente o en el futuro se hace de dominio público sin culpa de ninguna de las partes,
- 3) Puede comprobarse que estaba en posesión de esa parte en el momento que fue divulgada y no fue previamente obtenida directa o indirectamente de la otra parte, o
- 4) Que de otra manera fue legalmente puesta a la disponibilidad de esa parte por un tercero que no tenía obligación de confidencialidad.

Las disposiciones precedentes no modificarán de ninguna manera ningún compromiso de confidencialidad otorgado por cualquiera de las partes a quien esto compete antes de la fecha del contrato con respecto a los suministros o cualquier parte de ellos.

Las disposiciones de esta cláusula permanecerán válidas después del cumplimiento o terminación del contrato por cualquier razón.

Obligatoriedad de declarar información del personal del proveedor, consultor o contratista en el SICP

1. El proveedor deberá proporcionar los datos de identificación de sus subproveedores, así como de las personas físicas por medio de las cuales propone cumplir con las obligaciones del contrato, dentro de los treinta días posteriores a la obtención del código de contratación, y con anterioridad al primer pago que vaya a percibir en el marco de dicho contrato, con las especificaciones respecto a cada una de ellas. A ese respecto, el contratista deberá consignar dichos datos en el Formulario de Identificación del Personal (FIP) y en el Formulario de Identificación de Servicios Personales (FIS), a través del Registro del Proveedor del Estado.
2. Cuando ocurra algún cambio en la nómina del personal o de los subcontratistas propuestos, el proveedor o contratista está obligado a actualizar el FIP.
3. Como requerimiento para efectuar los pagos a los proveedores o contratistas, la contratante, a través del procedimiento establecido para el efecto por la entidad previsional, verificará que el proveedor o contratista se encuentre al día en el cumplimiento con sus obligaciones para con el Instituto de Previsión Social (IPS).
4. La contratante podrá realizar las diligencias que considere necesarias para verificar que la totalidad de las personas que prestan servicios personales en relación de dependencia para la contratista y eventuales subcontratistas se encuentren debidamente individualizados en los listados recibidos.

5. El proveedor o contratista deberá permitir y facilitar los controles de cumplimiento de sus obligaciones de aporte obrero patronal, tanto los que fueran realizados por la contratante como los realizados por el IPS, y por funcionarios de la DNCP. La negativa expresa o tácita se considerará incumplimiento del contrato por causa imputable al proveedor o contratista.

6. En caso de detectarse que el proveedor o contratista o alguno de los subcontratistas, no se encontraran al día con el cumplimiento de sus obligaciones para con el IPS, deberán ser emplazados por la contratante para que en diez (10) días hábiles cumplan con sus obligaciones pendientes con la previsual. En el caso de que no lo hiciera, se considerará incumplimiento del contrato por causa imputable al proveedor o contratista.

Porcentaje de Garantía de Fiel Cumplimiento de Contrato

El Porcentaje de Garantía de Fiel Cumplimiento de Contrato es de:

10,00 %

El proveedor debe presentar esta garantía dentro de los 10 días corridos siguientes a la fecha de suscripción del contrato.

Forma de Instrumentación de Garantía de Fiel Cumplimiento de Contrato

La garantía de fiel cumplimiento de contrato adoptará alguna de las siguientes formas: Garantía bancaria o Póliza de Seguros.

Periodo de validez de la Garantía de Cumplimiento de Contrato

El plazo de vigencia de la Garantía de Fiel Cumplimiento de Contrato será (en días corridos) de:

Desde la firma del contrato y por todo el periodo de la ejecución, más un periodo de 30 días calendario posteriores al vencimiento del mismo

Si la entrega de los bienes o la prestación de los servicios, se realizare en un plazo menor o igual a diez (10) días corridos posteriores a la firma del contrato, la garantía de fiel cumplimiento deberá ser entregada antes del cumplimiento de la prestación.

Una vez cumplidas las obligaciones por parte del proveedor o contratista, la Garantía de Fiel Cumplimiento de Contrato podrá ser liberada y devuelta al proveedor, a requerimiento de parte, dentro de los treinta (30) días contados a partir de la fecha de cumplimiento de las obligaciones, incluyendo cualquier obligación relativa a la garantía de los bienes y/o servicios.

Formas y condiciones de pago

El adjudicado para solicitar el pago de las obligaciones deberá presentar la solicitud acompañada de los siguientes documentos:

1. Documentos Genéricos:

- a. Nota de remisión u orden de prestación de servicios según el objeto de la contratación;
- b. La factura de pago, con timbrado vigente, la cual deberán expresar claramente por separado el Impuesto al Valor Agregado (IVA) de conformidad con las disposiciones tributarias aplicables. En ningún caso el valor total facturado podrá exceder el valor adjudicado o las adendas aprobadas;
- c. REPSE (registro de prestadores de servicios) todos los que son prestadores de servicios;
- d. Certificado de Cumplimiento Tributario;
- e. Constancia de Cumplimiento con la Seguridad Social;
- f. Formulario de Identificación de Servicios Personales (FIS);
- g. Certificado laboral vigente expedido por la Dirección de Obrero Patronal dependiente del Viceministerio de Trabajo, siempre que el sujeto esté obligado a contar con el mismo, de conformidad a la reglamentación pertinente - CPS

Otras formas y condiciones de pago al proveedor en virtud del contrato serán las siguientes:

Los pagos se harán efectivos dentro de los 60 (sesenta) días calendarios posteriores a la presentación de las solicitudes respectivas a la Gerencia Económica, previa verificación de su correcta presentación y procesamiento de la misma.

El Pago correspondiente al Ejercicio Fiscal 2025 será conforme al monto previsto en la Disponibilidad Presupuestaria del presente llamado.

El pago correspondiente para el Ejercicio Fiscal 2026 estará sujeto a disponibilidad presupuestaria.

De las facturas presentadas se efectuará un descuento del 0.4% (cero punto cuatro por ciento), en concepto de Contribución sobre Contratos Suscritos, a fin de dar cumplimiento a lo establecido en el Art. 63 de la Ley N° 7021/22.

2. La Contratante efectuará los pagos, dentro del plazo establecido en este apartado, sin exceder sesenta (60) días después de la presentación de una factura por el proveedor. La contratante deberá expedirse respecto a la aceptación o rechazo de la factura, a más tardar en quince (15) días corridos posteriores a su presentación.

3. De conformidad a las disposiciones del Decreto N° 7781/2006, del 30 de junio de 2006 y modificatoria, en las contrataciones con Organismos de la Administración Central, el proveedor deberá habilitar su respectiva cuenta corriente o caja de ahorro en un Banco de plaza y comunicar a la Contratante para que ésta gestione ante la Dirección General del Tesoro Público, la habilitación en el Sistema de Tesorería (SITE).

El certificado previsto en el inciso g), se requerirá únicamente para el último pago.

Solicitud de suspensión de la ejecución del contrato

Si la mora en el pago por parte de la contratante fuere superior a sesenta (60) días corridos, el proveedor, consultor o contratista, tendrá derecho a solicitar por escrito la suspensión de la ejecución del contrato por causas imputables a la contratante.

La solicitud deberá ser respondida por la contratante dentro de los 10 (diez) días hábiles de haber recibido por escrito el requerimiento. Pasado dicho plazo sin respuesta se considerará denegado el pedido, con lo que se agota la instancia administrativa quedando expedita la vía contencioso administrativa.

Si la demora en el pago fuese superior a ciento veinte (120) días corridos, el proveedor, consultor o contratista podrá

proceder a la suspensión del cumplimiento del contrato, debiendo comunicar a la contratante con un mes de antelación tal circunstancia, a efectos del reconocimiento de los derechos que puedan derivarse de dicha suspensión, en los términos establecidos en la Ley. En este supuesto, el pago total de lo adeudado por la contratante determinará la continuidad del cumplimiento del contrato.

Anticipo MIPYMES

Se otorgará Anticipo MIPYMES:

No Aplica

Solicitud de Pago de Anticipo

El plazo dentro del cual se solicitará el anticipo será (en días corridos) de:

No Aplica

Forma de Instrumentación de Garantía de anticipo

Indicar en este apartado la forma de instrumentar la garantía de anticipo.

No Aplica

Reajuste

El precio del contrato estará sujeto a reajustes. La fórmula y el procedimiento para el reajuste serán los siguientes:

La fórmula y el procedimiento para el reajuste serán los siguientes: siempre y cuando la variación del IPC publicado por el Banco Central del Paraguay (BCP) haya sufrido una variación igual o mayor al 15% (quince por ciento) referente a la fecha de apertura de ofertas

$Pr = P \times \frac{IPC_1}{IPC_0}$

IPC0

Dónde:

Pr: Precio Reajustado.

P: Precio adjudicado.

IPC1: Índice de precios al Consumidor publicado por el Banco Central del Paraguay, correspondiente al mes de la entrega del suministro.

IPC0: Índice de precios al consumidor publicado por el Banco Central del Paraguay, correspondiente al mes de la apertura de ofertas.

Los reajustes deberán ser solicitados por escrito al SNPP, por el Proveedor.

La solicitud debe realizarse indefectiblemente dentro del mes siguiente al cual se produjeron las variaciones.

No se reconocerán reajustes de precios si los servicios se encuentran atrasados respecto al cronograma de entrega.

La variación del valor del contrato por reajuste de precios, no constituye modificación del contrato en los términos de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas", sin embargo, deberá contar con un Código de Contratación, para cuya obtención se deberá cumplir con los requerimientos establecidos por la DNCP.

Porcentaje de multas

El valor del porcentaje de multas que será aplicado por el atraso en la entrega de los bienes, prestación de servicios será de:

0,50 %

La contratante podrá deducir en concepto de multas una suma equivalente al porcentaje del precio de entrega de los bienes atrasados, por cada día de atraso indicado en este apartado.

La aplicación de multas no libera al proveedor del cumplimiento de sus obligaciones contractuales.

Tasa de interés por Mora

En caso de que la contratante incurriera en mora en los pagos, se aplicará una tasa de interés por cada día de atraso, del:

0,01

En ningún caso el porcentaje podrá superar al tope máximo definido en la Resolución MEF N° 12/2025, en cuyo supuesto, se aplicará un ajuste automático al contrato con los topes respectivos, de conformidad a las reglas establecidas en la mencionada resolución, según se traten de contratos en guaraníes o en dólares estadounidenses.

La mora será computada a partir del día siguiente del vencimiento del pago y no incluye el día en el que la contratante realiza el pago.

Si la contratante no efectuara cualquiera de los pagos al proveedor en las fechas de vencimiento correspondiente, la contratante

pagará al proveedor interés sobre los montos de los pagos morosos a la tasa establecida en este apartado, por el período de la demora hasta que haya efectuado el pago completo, ya sea antes o después de cualquier juicio.

Si la mora fuera superior a 60 días, el proveedor, consultor o contratista tendrá derecho a la suspensión del contrato, por motivos que no le serán imputables, previa comunicación a la contratante, de acuerdo a lo establecido en el artículo 66 de la Ley N° 7021/22.

Impuestos y derechos

En el caso de bienes de origen extranjero, el proveedor será totalmente responsable del pago de todos los impuestos, derechos, gravámenes, timbres, comisiones por licencias y otros cargos similares que sean exigibles fuera y dentro de la República del Paraguay, hasta el momento en que los bienes contratados sean entregados al contratante.

En el caso de origen nacional, el proveedor será totalmente responsable por todos los impuestos, gravámenes, comisiones por licencias y otros cargos similares incurridos hasta el momento en que los bienes contratados sean entregados a la contratante.

El proveedor será responsable del pago de todos los impuestos y otros tributos o gravámenes con excepción de los siguientes:

No Aplica

Convenios Modificatorios

La contratante podrá acordar modificaciones al contrato conforme al artículo N° 67 de la Ley N° 7021/22 “De Suministro y Contrataciones Públicas”.

1. Cuando el sistema de adjudicación adoptado sea de abastecimiento simultáneo las ampliaciones de los contratos se registrarán por las disposiciones contenidas en la Ley N° 7021/22, sus modificaciones y reglamentaciones, que para el efecto emita la DNCP.
 2. Tratándose de contratos abiertos, las modificaciones a ser introducidas se registrarán atendiendo a la reglamentación vigente.
 3. La celebración de un convenio modificatorio conforme a las reglas establecidas en el artículo N° 67 de la Ley N° 7021/22, que constituyan condiciones de agravación del riesgo cuando la Garantía de Cumplimiento de Contrato sea formalizada a través de póliza de seguro, obliga al proveedor a informar a la compañía aseguradora sobre las modificaciones a ser realizadas y en su caso, presentar ante la contratante los endosos por ajustes que se realicen a la póliza original en razón al convenio celebrado con la contratante.

Limitación de responsabilidad

Excepto en casos de negligencia grave o actuación de mala fe, el proveedor no tendrá ninguna responsabilidad contractual de agravio o de otra índole frente a la contratante por pérdidas o daños indirectos o consiguientes, pérdidas de utilización, pérdidas de producción, o pérdidas de ganancias o por costo de intereses, estipulándose que esta exclusión no se aplicará a ninguna de las obligaciones del proveedor de pagar a la contratante las multas previstas en el contrato.

Responsabilidad del proveedor

El proveedor deberá suministrar todos los bienes o servicios de acuerdo con las condiciones establecidas en el pliego de bases y condiciones, sin perjuicio de las responsabilidades establecidas en la Ley N° 7021/22.

Fuerza mayor

El proveedor no estará sujeto a la ejecución de su Garantía de Cumplimiento, liquidación por daños y perjuicios o terminación por incumplimiento en la medida en que la demora o el incumplimiento de sus obligaciones en virtud del contrato sea el resultado de un evento de Fuerza Mayor.

1. Para fines de esta cláusula, "Fuerza Mayor" significa un evento o situación fuera del control del proveedor que es imprevisible, inevitable y no se origina por descuido o negligencia del mismo. Tales eventos pueden incluir sin que éstos sean los únicos actos de la autoridad en su capacidad soberana, guerras o revoluciones, incendios, inundaciones, epidemias, pandemias, restricciones de cuarentena, y embargos de cargamentos.
2. El proveedor deberá demostrar el nexo existente entre el caso notorio y la obligación pendiente de cumplimiento. La fuerza mayor solamente podrá afectar a la parte del contrato cuyo cumplimiento imposible fue probado.
3. No se considerarán casos de Fuerza Mayor los actos o acontecimientos que hagan el cumplimiento de una obligación únicamente más difícil o más onerosa para la parte correspondiente.
4. Si se presentara un evento de Fuerza Mayor, el proveedor notificará por escrito a la contratante sobre dicha condición y causa, en el plazo de siete (7) días calendario a partir del día siguiente en que el proveedor haya tenido conocimiento del evento o debiera haber tenido conocimiento del evento. Transcurrido el mencionado plazo, sin que el proveedor o contratista haya notificado a la convocante la situación que le impide cumplir con las condiciones contractuales, no podrá invocar caso fortuito o fuerza mayor. Excepcionalmente, la convocante bajo su responsabilidad, podrá aceptar la notificación del evento de caso fortuito en un plazo mayor, debiendo acreditar el interés público comprometido.
5. La fuerza mayor debe ser invocada con posterioridad a la suscripción del contrato y con anterioridad al vencimiento del plazo de cumplimiento de las obligaciones contractuales.

A menos que la contratante disponga otra cosa por escrito, el proveedor continuará cumpliendo con sus obligaciones en virtud del contrato en la medida que sea razonablemente práctico, y buscará todos los medios alternativos de cumplimiento que no estuviesen afectados por la situación de fuerza mayor existente.

Causales de terminación del contrato

1. Terminación por Incumplimiento

a) La contratante, sin perjuicio de otros recursos a su disposición en caso de incumplimiento del contrato, podrá terminar el contrato, en cualquiera de las siguientes circunstancias:

- i. Si el proveedor no entrega parte o ninguno de los bienes dentro del período establecido en el contrato, o dentro de alguna prórroga otorgada por la contratante; o
- ii. Si el proveedor no cumple con cualquier otra obligación en virtud del contrato; o
- iii. Si el proveedor, a juicio de la contratante, durante el proceso de licitación o de ejecución del contrato, ha participado en actos de fraude y corrupción;
- iv. Cuando las multas por atraso superen el monto de la Garantía de Cumplimiento de Contrato;
- v. Por suspensión de los trabajos, imputable al proveedor o al contratista, por más de sesenta días calendarios, sin que

- medie fuerza mayor o caso fortuito;
vi. En los demás casos previstos en este apartado.

2. Terminación por insolvencia o quiebra

La contratante podrá terminar el contrato mediante comunicación por escrito al proveedor si éste se declarase en quiebra o en estado de insolvencia.

3. Terminación por conveniencia

a) La contratante podrá en cualquier momento terminar total o parcialmente el contrato por razones de interés público debidamente justificada, mediante notificación escrita al proveedor. La notificación indicará la razón de la terminación, así como el alcance de la terminación con respecto a las obligaciones del proveedor, y la fecha en que se hace efectiva dicha terminación.

b) Los bienes que ya estén fabricados y estuviesen listos para ser enviados a la contratante dentro de los treinta (30) días siguientes a la fecha de recibo de la notificación de terminación del contrato deberán ser aceptados por la contratante de acuerdo con los términos y precios establecidos en el contrato. En cuanto al resto de los bienes la contratante podrá elegir entre las siguientes opciones:

-Que se complete alguna porción y se entregue de acuerdo con las condiciones y precios del contrato; y/o

-Que se cancele la entrega restante y se pague al proveedor una suma convenida por aquellos bienes que hubiesen sido parcialmente completados y por los materiales y repuestos adquiridos previamente por el proveedor.

Se podrán establecer otras causales de terminación de contrato, de acuerdo a su naturaleza, y se deberán tener en cuenta además, las previstas en el artículo 72 y concordantes de la Ley N° 7021/22.

Otras causales de terminación del contrato

Además de las ya indicadas en la cláusula anterior, otras causales de terminación de contrato son:

No Aplica

Fraude y Corrupción

1. La convocante exige que los participantes en los procedimientos de contratación, observen los más altos niveles éticos, ya sea durante el proceso de licitación o de ejecución de un contrato. La convocante actuará frente a cualquier hecho o reclamación que se considere fraudulento o corrupto.

2. Si se comprueba que un funcionario público, o quien actúe en su lugar, y/o el oferente o adjudicatario propuesto en un proceso de contratación, hayan incurrido en prácticas fraudulentas o corruptas, la convocante deberá:

(i) En la etapa de oferta, se descalificará cualquier oferta del oferente y/o rechazará cualquier propuesta de adjudicación relacionada con el proceso de adquisición o contratación de que se trate; y/o

(ii) Durante la ejecución del contrato, se rescindirá el contrato por causa imputable al proveedor;

(iii) Se remitirán los antecedentes del oferente o proveedor directamente involucrado en las prácticas fraudulentas o corruptivas, a la Dirección Nacional de Contrataciones Públicas, a los efectos de la aplicación de las sanciones previstas.

(iv) Se presentará la denuncia ante las instancias correspondientes si el hecho conocido se encontrare tipificado en la legislación penal.

Fraude y corrupción comprenden actos como:

- (i) Ofrecer, dar, recibir o solicitar, directa o indirectamente, cualquier cosa de valor para influenciar las acciones de otra parte;
- (ii) Cualquier acto u omisión, incluyendo la tergiversación de hechos y circunstancias, que engañen, o intenten engañar, a alguna parte para obtener un beneficio económico o de otra naturaleza o para evadir una obligación;
- (iii) Perjudicar o causar daño, o amenazar con perjudicar o causar daño, directa o indirectamente, a cualquier parte o a sus bienes para influenciar las acciones de una parte;
- (iv) Colusión o acuerdo entre dos o más partes realizado con la intención de alcanzar un propósito inapropiado, incluyendo influenciar en forma inapropiada las acciones de otra parte.
- (v) Cualquier otro acto considerado como tal en la legislación vigente.

3. Los oferentes deberán declarar que por sí mismos o a través de interpósita persona, se abstendrán de adoptar conductas orientadas a que los funcionarios o empleados de la convocante induzcan o alteren las evaluaciones de las propuestas, el resultado del procedimiento u otros aspectos que les otorguen condiciones más ventajosas con relación a los demás participantes.

Medio alternativo de Resolución de Conflictos a través del Avenimiento.

“Los contratistas, proveedores, consultores y contratantes, podrán solicitar la intervención de la Dirección Nacional de Contrataciones Públicas alegando el incumplimiento de los términos y condiciones pactados en los contratos regidos por la Ley N° 7021/22. Una vez recibida la solicitud respectiva, dentro de los 15 (quince) días hábiles siguientes a la fecha de su recepción, la Dirección Nacional de Contrataciones Públicas señalará día y hora para audiencia de avenimiento a la que serán citadas las partes. Los requisitos y formalidades para admitir o rechazar la solicitud de intervención, así como los demás trámites del procedimiento de avenimiento serán dispuestos en la reglamentación. Serán aplicables al procedimiento de Avenimiento las disposiciones contenidas en la sección I del Capítulo XVI “PROCEDIMIENTOS JURIDICOS SUSTANCIADOS ANTE LA DIRECCIÓN NACIONAL DE CONTRATACIONES PÚBLICAS” de la Ley N° 7021/22.

Medio Alternativo de Resolución de Conflictos a través de la Mediación

El procedimiento de Mediación se podrá llevar a cabo ante:

No Aplica

El mediador deberá pertenecer a las Listas del Poder Judicial o del CAMP, según la selección de sede establecida.

Medio alternativo de Resolución de Conflictos a través del Arbitraje

El procedimiento arbitral se podrá llevar a cabo ante las sedes del Centro de Arbitraje y Mediación del Paraguay (en adelante, "CAMP"). El tribunal será conformado por:

No Aplica

MODELO DE CONTRATO

Este modelo de contrato, constituye la proforma del contrato a ser utilizado una vez adjudicado al proveedor y en los plazos dispuestos para el efecto por la normativa vigente.

EL MODELO DE CONTRATO SE ENCUENTRA EN UN ARCHIVO ANEXO A ESTE DOCUMENTO.

FORMULARIOS

Los formularios dispuestos en esta sección son los estándar a ser utilizados por los potenciales oferentes para la preparación de sus ofertas.

ESTA SECCIÓN DE FORMULARIOS SE ENCUENTRA EN UN ARCHIVO ANEXO A ESTE DOCUMENTO, DEBIENDO LA CONVOCANTE MANTENERLO EN FORMATO EDITABLE A FIN DE QUE EL OFERENTE LO PUEDA UTILIZAR EN LA PREPARACION DE SU OFERTA.

