REPÚBLICA DEL PARAGUAY

PLIEGO DE BASES Y CONDICIONES

Convocante:

Comisión Nacional de Telecomunicaciones (CONATEL)

Uoc Conatel

Nombre de la Licitación:

SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN Y CONTROLES CRITICOS DE CIBERSEGURIDAD

(versión 3)

ID de Licitación:

477705

Modalidad:

Licitación Pública Nacional

Publicado el:

02/11/2026

"Pliego para la Adquisición de Bienes y/o Servicios - CONVENCIONAL - Ley Nº 7021/22."

Versión 4

RESUMEN DEL LLAMADO

Datos de la Convocatoria

ID de Licitación:	477705	**Nombre de la Licitación:**	SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN Y CONTROLES CRITICOS DE CIBERSEGURIDAD
Convocante:	Comisión Nacional de Telecomunicaciones (CONATEL)	**Categoría:**	43000000 - Tecnologias de Informacion, Telecomunicaciones y Radiodifusiones
Unidad de Contratación:	Uoc Conatel	**Tipo de Procedimiento:**	LPN - Licitación Pública Nacional

Características Especiales de la Convocatoria

Etapas y Plazos

Lugar para Realizar Consultas:	Consultas a travez del Portal	**Fecha Límite de Consultas:**	11/09/2026 12:00
Lugar de Entrega de Ofertas:	Presidente Franco 780 esq. Ayolas -edificio Ayfra -Piso 3	**Fecha de Entrega de Ofertas:**	11/11/2026 08:45
Lugar de Apertura de Ofertas:	Presidente Franco 780 esq. Ayolas -edificio Ayfra -Piso 3	**Fecha de Apertura de Ofertas:**	11/11/2026 09:00

Adjudicación y Contrato

Sistema de Adjudicación:	Total	**Anticipo:**	20.0%
Vigencia del Contrato:	31/12/2028		

Datos del Contacto

Nombre:	Abg. Hugo Balbuena Villate	**Cargo:**	Gerente de la Gerencia Operativa de Contrataciones
Teléfono:	4382401	**Correo Electrónico:**	danielbalbuena@conatel.gov.py

ADENDA

Adenda

Las modificaciones al presente procedimiento de contratación son los indicados a continuación:

Asunción, 29 de octubre de 2026.

REF: *LICITACION PUBLICA NACIONAL N° 15/2026- SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION Y CONTROLES CRITICOS DE CIBERSEGURIDAD- ID N° 477.705*

La Gerencia Operativa de Contrataciones de la Comisión Nacional de Telecomunicaciones (CONATEL), comunica la modificación en el Sistema de Información de Contrataciones Públicas (SICP), de acuerdo al siguiente detalle y a la resulta de la protesta RESOLUCION DNCP 3074/2026:

1) **SE MODIFICA** la fecha de entrega y apertura de ofertas.

ABG. HUGO DANIEL BALBUENA VILLATE

GERENTE

GERENCIA OPERATIVA DE CONTRATACIONES

La adenda es el documento emitido por la convocante, mediante la cual se modifican aspectos establecidos en las bases de la contratación. A los efectos legales, la adenda será considerada parte integrante del documento cuyo contenido modifique.

La convocante podrá introducir modificaciones cuando se ajuste a los parámetros establecidos en la Ley.

Las adendas serán difundidas en el SICP respetando los plazos establecidos en la resolución por la cual se Reglamentan los Procedimientos de Contratación regidos por la Ley N° 7021/22.

Obs: Cuando la convocante requiera prorrogar la fecha tope de presentación y apertura de ofertas, sin modificar los demás datos e información de las bases de la contratación, será difundida automáticamente a través del SICP y no se instrumentará a traves de adenda.

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 Sostenible - 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, por medio de prácticas como la modificación de los procesos de producción, manutención y mantenimiento de equipos y gestión de las instalaciones, así como 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 por las convocantes 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

Cuando se admitiera la presentación de anexos técnicos y folletos en idioma distinto al español, su traducción deberá ser realizada por un traductor público matriculado en la República del Paraguay.

Lista de Precios

Cuando la presentación de la oferta se realice a través del módulo de oferta electrónica, se considerará que el listado de ítems forma parte del formulario de oferta electrónico, y deberá sujetarse en todo lo demás a la reglamentación vigente.

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 a la planilla de precios.

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 a la planilla de precios.

e) En todos los casos, independientemente 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 multiplicando 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 simultaneo, en este apartado se deberá indicar la manera de distribución de los mismos:

No Aplica

Supuesto de abastecimiento simultáneo

El abastecimiento se regirá por el supuesto de:

No Aplica

Moneda de la oferta y pago

La moneda de la oferta y pago será:

Moneda Nacional

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.

Moneda extranjera

La moneda extranjera para la oferta y pago, será:

No Aplica

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:

1 copia

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 se admitirá la presentación de la constancia de perfil del proveedor. El proveedor deberá proceder a la vinculación de los documentos del Registro de Proveedores del Estado a través del Módulo de Ofertas Electrónicas, según lo dispuesto en las disposiciones vigentes.

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

Una oferta alternativa se configura necesariamente con la presentación de la oferta principal, que se ajuste a las condiciones previstas en las bases y condiciones; y, de manera separada e independiente una propuesta alternativa, que implique alternativas técnicas a los requerimientos de la licitación y cuya consideración estaría sujeta a que dicha alternativa reúna mejores condiciones de oportunidad, calidad y costo.

Periodo de validez de las ofertas

Las ofertas deberán mantenerse válidas por:

53

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 a los oferentes la extensión del periodo de validez de la oferta. En caso de aceptar dicha solicitud, el oferente deberá manifestar su consentimiento de forma expresa, y, en consecuencia, prorrogar igualmente la Garantía de Mantenimiento de la Oferta.

El oferente podrá rechazar la solicitud de prórroga sin que ello implique la ejecución de su Garantía de Mantenimiento de la Oferta. En caso de aceptar la extensión solicitada, no se le pedirá ni se le permitirá modificar su oferta.

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, siempre y cuando sea de fecha previa a la presentación y apertura de sobres.
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 contratos abiertos, el porcentaje de las garantías a ser presentado por los oferentes que participen, deberá ser aplicado sobre el monto máximo total del llamado; si la adjudicación fuese por lote o ítem ofertado, deberán sumarse los valores máximos de cada lote o ítem ofertado, o de la suma de los valores máximos obtenidos por la multiplicación de los precios unitarios ofertados con las cantidades máximas, a fin de obtener el monto sobre el cual se aplicará el porcentaje de la citada garantía.

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,

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

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

g. Si el adjudicatario no presentare las legalizaciones correspondientes para la firma del contrato, cuando éstas sean requeridas.

La Garantía de Mantenimiento de Oferta, sea cual fuere la forma de instrumentación adoptada, cuando se tenga acreditada una de las causales de ejecución de la garantía deberá ser pagadera según el tipo de garantía que haya sido solicitada.

Periodo de Validez de la Garantía de Mantenimiento de Oferta

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

90

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.

Condiciones especiales de la Garantía de Mantenimiento de Oferta

Las condiciones especiales de la Garantía de Mantenimiento de Oferta serán:

No Aplica

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° 7021/22.

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 regirá por las disposiciones establecidas en la normativa vigente y la guía de ofertas electrónicas.

Cuando el sobre no cuente con el RUC, se podrá subsanar dicha omisión al momento de la presentación.

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 inscriptos en el Registro de Proveedores del Estado conforme con los datos previstos en el sobre, en caso de que, no sea posible identificar al oferente mediante el sobre presentado, la UOC procederá a abrirlo con el fin de verificar el número de RUC incluido entre los documentos de la oferta, para constatar si el oferente se encuentra inscripto en el Registro de Proveedores del Estado. En caso de que el oferente no inscripto en el Registro haya presentado la oferta, la convocante deberá dejar constancia en el acta de apertura electrónica.

La oferta del oferente no inscripto que cuente con la identificación de RUC en el sobre, no será abierta sino devuelto al oferente remitente. La oferta del oferente que no cuente con la identificación de RUC en el sobre será abierta y remitida al órgano evaluador de la convocante, para la evaluación de la oferta o su rechazo, según corresponda.

La presente disposición será aplicable en los procedimientos de doble sobre en los que será abierta la oferta técnica para la verificación respectiva, siempre y cuando la misma esté debidamente identificada como sobre técnico.

Esta disposición no será aplicable a los procedimientos que utilicen el módulo de ofertas electrónicas y a aquellos procedimientos especiales que, por su naturaleza, expresamente no requieran de la inscripción en el Registro de Proveedores del Estado como condición de participación.

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. El acta se difundirá a través del SICP.

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. 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.

1.9. 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:

SI APLICA. Autorización del Representante o Distribuidor de la marca ofertada para los ítems 1, 2 y 3 . 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. Las mismas deberán ser presentadas en el momento determinado en este apartado. La falta de presentación de las muestras en tiempo y condiciones 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:

10 (diez) días hábiles contados desde la fecha de notificación del Administrador de Contrato. -.

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:

Veinticuatro (24) meses, contados desde el Acta de Conformidad de recepción de los bienes.

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 guaranies, contra riesgo de extravío o daños incidentales ocurridos durante la fabricación, adquisición, transporte, almacenamiento y entrega, de acuerdo a los incoterms aplicables.

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.

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’’.

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, inscriptos 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.

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.

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 Nº 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 Nº 7021/22, el comité de evaluación realizará el siguiente análisis:

1º 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.

2º 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 incursos en las causales previstas en los Arts. 17 y 21 de la Ley Nº 7021/22.

3º 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.

4º Si se constatara 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.

5º 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 la empresa, 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.

6º 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.

7º 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 Nº 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 Nº 7021/22, pudiendo 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.

Método de Evaluación

Basado únicamente en precio

En caso de optar por el método de multiplicidad de criterios deberá estar supeditado a los lineamientos emitidos por el MEF y la DNCP.

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, cuando los montos cotizados se aparten de los parámetros o rangos establecidos en la normativa aplicable.

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:

Utilidad, impuestos, insumos, costos, mano de obra y gastos administrativos.

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 normativa aplicable.

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, el oferente podrá complementar 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.

b) Oferentes en Consorcio:

b.1. Provisión de Bienes. El CPEN debe ser expedido a nombre del miembro, o los miembros, que fabrique o produzca los bienes objeto de la contratación. En el caso que ninguno de los integrantes del consorcio 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 constituido o en formación, o a nombre de cualquiera de los integrantes del mismo.

b.2. Provisión de Servicios. Todos los integrantes del consorcio deben contar con el CPEN. (Se entenderá por el término “servicio” aquello que comprende a los servicios en general, las consultorías, obras públicas y servicios relacionados a obras públicas).

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 específico certificado.

Para los casos de prestación de servicios, el CPEN será intransferible. Se permite el uso del CPEN por terceros 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.

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

Margen de preferencia en procedimientos de contratación de carácter internacional

No Aplica

Requisitos documentales para la evaluación de las condiciones de participación.

1. Formulario de Oferta (*) *[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.]*
2. Garantía de Mantenimiento de Oferta (*) *[La garantía de mantenimiento de oferta debe ser extendida, bajo la forma establecida en el SICP.*
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 profesional, comercial y/o industrial 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, y deberán estar vigente a la fecha y hora tope de presentación de oferta.

Los documentos indicados con doble asterisco (**) son considerados documentos formales y deben 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 disconformidad 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 o cuando el titular de una empresa no sea empleador, 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. ***contribuyente de IRACIS/IRE.***

Deberán cumplir con el siguiente parámetro:

a.1. ***Ratio de Liquidez:*** *activo corriente / pasivo corriente*

Deberá ser igual o mayor que 1, en promedio, en los 3 (tres) años de ejercicios cerrados (2023,2024,2025)

a.2. Endeudamiento: *pasivo total / activo total*

No deberá ser mayor a 0,80 en promedio, en los 3 (tres) años de ejercicios cerrados (2023,2024,2025)

a.3 Rentabilidad: *Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital.*

El promedio en los en los 3 (tres) últimos años (2023,2024,2025) no deberá ser negativo de ejercicios cerrados.

b) contribuyentes de IRE SIMPLE

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales requeridos (2023,2024,2025)

c) contribuyentes de IRP

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales requeridos (2023,2024,2025)

d) contribuyentes de exclusivamente IVA General

Deberá cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales (2023,2024,2025)

En caso de consorcios, el líder deberá cumplir con el 60% y el 40% restante de los requisitos los demás miembros del consorcio. -

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 Resultados de los años (2023,2024,2025)]
b. [Formulario 500 para los años (2023,2024,2025)]) correspondientes a la Declaración Jurada del Impuesto a la Renta]
c. [Formulario 501 para los años 2023,2024,2025)]correspondientes a Contribuyentes del IRE SIMPLE]
d. [Formulario 515 para Contribuyentes de Renta Personal y Formulario 516 IRP RCG de los años 2023,2024,2025)]]
e. Formulario 120 de los años 2023,2024,2025)]para contribuyentes del IVA.

Experiencia requerida

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

1. Demostrar experiencia en **servicios de diseño, implementación y operación de SOC** con contratos y/o facturaciones de venta y/o recepciones finales tanto a empresas publicas y/o privadas por un monto equivalente al 50% como mínimo del monto total ofertado en la presente licitación, de los últimos 3 años: 2023, 2024, 2025. Las sumatorias de las facturaciones deben alcanzar el porcentaje indicado, no será necesaria la presentación del porcentaje del monto establecido por cada año.
2. Se requiere que la empresa cuente con certificación ISO 27001
3. La empresa deberá tener una antigüedad mínima en el mercado, de por lo menos 5 (cinco) años en el rubro TICs.

En caso de consorcios, el líder deberá cumplir con el 60% y el 40% restante de los requisitos los demás miembros del consorcio.

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 facturaciones, contratos y/o recepciones finales que avalen la experiencia requerida.

1. **Copia de contratos y/o facturaciones y/o recepciones finales que avalen la experiencia requerida.**
2. **Copia Simple de la Certificación ISO 27001 Vigente.**
3. **Constancia de RUC.**

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, la patente municipal o los documentos constitutivos, 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:

1. El oferente deberá demostrar:
    a. **Domicilio legal y SOC en territorio paraguayo:** El oferente deberá contar con una oficina operativa y un Centro de Operaciones de Seguridad (SOC) activo, ambos con domicilio legal en la República del Paraguay, y ambos operativos al momento de la presentación de la oferta.
    b. **Características mínimas del SOC:**
        i. Monitoreo contínuo (24x7) de eventos de seguridad.
        ii. Capacidad para gestionar como mínimo 1.000 activos (endpoints o servidores).
        iii. Registro comercial vigente (patente municipal).
        iv. 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 32 meses.
2. Personal Técnico Requerido
    a. **Técnicos de Monitoreo SOC**: Al menos dos (2) técnicos con experiencia mínima de 2 años en ciberseguridad.
    b. **Lider de Proyecto**: Un (1) líder de proyecto con experiencia mínima de quince (15) años en Seguridad de la Información con experiencia en el desarrollo de procedimientos relacionados al SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), con las siguientes funciones:

- Diseñar e implementar marcos de gobernanza de riesgos alineados con la estrategia y apetito de riesgo de la organización.
- Definir roles, responsabilidades y estructuras de gobierno (comités de riesgos, propietarios de activos/riesgos).
- Elaborar políticas, procedimientos y directrices para la gestión integral de riesgos TI.
- Asegurar comunicación y reporte periódicas sobre el estado de los riesgos y su impacto en la organización.

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 vigente - Certificación en Auditoría de Sistemas y/o Seguridad de la Información vigente - Certificación en Auditoría ISO/IEC 27001 (40hs o más) vigente. - Certificación en Seguridad de Información y/o Continuidad de Negocio vigente. - Diplomado en Gestión y dirección de proyectos	15 años en seguridad de la información	5 años en áreas como gestión de riesgos TI, auditoría interna/externa de TI, seguridad de la información ISO 27000, cumplimiento normativo o consultoría especializada	Exigido

Implementación de Solución	1	- Egresado de las carreras Ingenieria en Informatica, Ingenieria en Sistemas Informáticos, Ingeniería en Electrónica, Licenciatura en Análisis de Sistemas Informáticos o Licenciatura en Ciencias de la computación. - Curso de seguridad de la información o curso de manejo de la información. - Curso MGCTI y/o SCRUM y/o PM4R y/o gestión de proyectos. - Certificación en el área de ciberseguridad como FCA, FCF o CCNA Security. - Curso en respuesta a incidentes, gestión de incidentes o gestión de crisis cibernética. - Al menos 3 talleres, cursos, entrenamientos, conferencias o congresos en Ciberseguridad y/o seguridad de la información y/o Hacking Ético.	8 años de experiencia en trabajos relacionados al campo de la ciberseguridad	6 años de experiencia en configuración de servidores, despliegue de herramientas	Exigido

Técnicos de 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	2 años en soporte ciberseguridad	1 año en monitoreo SOC (análisis de logs, respuesta a incidentes)	Exigido

Todo el plantel propuesto deberá figurar en la planilla de IPS con una antigüedad mínima de 6 meses.

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.**
b. **Al menos tres (3) certificados o constancias contractuales o cartas de referencia que acrediten la operación del SOC durante los últimos 32 meses.**
c. **Presentar copia de planilla de IPS de los perfiles presentados, acompañado del respectivo Currículum Vitae, certificados de capacitaciones y/o constancias que avalen la experiencia para cada perfil**

Otros criterios que la convocante requiera

Otros criterios para la evaluación de las ofertas a ser considerados en ésta contratación serán:

No Aplica

Evaluación basada en multiplicidad de criterios

Se deben establecer los criterios de evaluación que serán aplicados al principio de valor por dinero, indicando por cada criterio la siguiente información:

No Aplica

En caso de optar por el método de multiplicidad de criterios deberá estar sujeto a los lineamientos emitidos por el MEF y la DNCP.

Ponderación de criterios de evaluación - Multiplicidad de criterios

La ponderación de cada criterio de evaluación especificado en la cláusula anterior será el siguiente:

No Aplica

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 aritmético.

El comité de evaluación deberá 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.
d. 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 comunicación 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 comunicación de los documentos en el SICP, comprenderá la Resolución del resultado y el informe de evaluación respectivo. La fecha de esta notificación se considera válida a todos los efectos, siempre que se cumplan con las formalidades previstas en el Art. 52 y 55 de la Ley N.º 7021/22 y, lo previsto en el Título V, Capítulo VI, Sección IV y V del Decreto Reglamentario N.º 2264/24.

En casos excepcionales, 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 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 comunicación 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 fecha prevista en 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 respecto al análisis de su oferta.

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 regirá 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:

- Identificar el nombre, cargo y la dependencia de la Institución de quien solicita el procedimiento de contratación a ser publicado. *Mag. Blas Enrique Espinoza Jefe del Departamento de Informática*
- Justificación de la necesidad que se pretende satisfacer mediante la contratación a ser realizada. ***La implementación de un Centro de Operaciones de Seguridad para ataques de Ciberseguridad es una inversión estratégica para CONATEL. Ayudará a identificar y abordar las debilidades de seguridad antes de que sean explotadas por atacantes, con lo que se protegerá nuestros activos digitales, la reputación de nuestra institución y la continuidad para el logro de metas y objetivos institucionales. A su vez, para proteger información personal y crítica, prevenir robos de identidad y evitar ataques informáticos como el ransomware. Garantiza la continuidad operativa de empresas, salvaguarda la reputación y asegura la confidencialidad, integridad y disponibilidad de los datos frente a amenazas constantes. Puntos clave sobre la importancia de la ciberseguridad: Protección de Datos Personales: Protege información confidencial contra robos, accesos no autorizados y fraudes. Continuidad del Negocio: Evita interrupciones operativas causadas por ataques cibernéticos, permitiendo que las empresas sigan funcionando. Confianza del Cliente: Implementar medidas de seguridad robustas genera confianza, esencial para la reputación de cualquier organización. Prevención de Ataques: Permite detectar y detener ciberataques, protegiendo sistemas, redes y dispositivos como computadoras y teléfonos móviles. Protección de Infraestructura: Es vital para salvaguardar servicios esenciales como energía y salud. Beneficios clave: Reducción de riesgos financieros: Evita las***

pérdidas económicas derivadas de robos de información. Seguridad en la red: Protege las conexiones y el almacenamiento en la nube. Mitigación de riesgos: Identifica vulnerabilidades y reduce el impacto de incidentes

- Justificación de la planificación, si se trata de un procedimiento de contratación periódico o sucesivo, o si el mismo responde a una necesidad temporal. *la presente contratación responde a una necesidad temporal debido a que es necesario identificar las debilidades de seguridad, es crucial para proteger los activos de datos críticos de una organización, asegurando su confidencialidad, integridad y disponibilidad frente a ciber amenazas. Permite gestionar riesgos de manera proactiva, garantizando la continuidad del negocio y el cumplimiento normativo. Importancia Clave del SGSI: Protección de Datos Sensibles: Salvaguarda la información crítica contra accesos no autorizados, alteraciones, pérdidas o destrucción. Gestión Proactiva de Riesgos: Identifica, evalúa y mitiga riesgos de seguridad mediante un enfoque estructurado (generalmente ISO/IEC 27001), reduciendo la probabilidad de incidentes. Continuidad del Negocio: Asegura que las operaciones esenciales continúen funcionando o se recuperen rápidamente tras un incidente, minimizando el impacto económico. Cumplimiento Legal y Normativo: Ayuda a cumplir con regulaciones de protección de datos (ej. RGPD) y normativas sectoriales, evitando sanciones económicas. Confianza y Reputación: Fortalece la reputación de la empresa y genera confianza en clientes, socios comerciales y proveedores al demostrar compromiso con la seguridad*

Las especificaciones técnicas deberán estar sustentadas en el dictamen técnico, requerido al momento de la comunicación de la convocatoria.

Especificaciones Técnicas "CPS"

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

El propósito de las 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. Siempre que sea posible deberán especificarse normas de calidad internacionales. 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 avales de funcionamiento cubiertas por la garantía, y las especificaciones de las multas aplicables en caso de que dichos avales 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:

ITEM 1 - Herramienta para monitoreo y remediación de vulnerabilidades para 500 dispositivos

N°	Descripción del Requerimiento	Exigido
PLATAFORMA		
	La plataforma debe ser Cloud - SaaS	Sí
	La plataforma debe tener visibilidad y cobertura en tiempo real para los sistemas operativos y aplicaciones de su organización, es decir, cualquier cambio en el inventario (instalación / desinstalación / cambio de aplicaciones y / o activos debe reflejarse instantáneamente en su panel de control)	Si
	La plataforma debe proporcionar una solución integrada para la gestión de vulnerabilidades, la priorización de riesgos y la corrección en una plataforma.	Sí
	La plataforma debe soportar alta disponibilidad	Sí

	La plataforma debe permitir instalar un proxy en la red para hacer patching caching	Sí
	El proxy debe ejecutarse en sistemas Linux Ubuntu o Red Hat	Sí
	El proxy no debe tener costo adicional	Sí
	Debe contar por lo menos con dos métodos de autenticación (Ej :User y pass, mail de verificación, SAML2 with IDPs)	Si
	La plataforma debe ofrecer mecanismos de protección para vulnerabilidades sin parches disponibles, aplicaciones heredadas o sistemas con ventanas de mantenimiento restringidas.	Si
	La plataforma debe ofrecer una única consola unificada para descubrimiento, priorización de riesgos, aplicación de parches, protección sin parches y ejecución de scripts, sin la necesidad de múltiples módulos o consolas adicionales.	Si
	La plataforma debe proporcionar KPI de exposición y remediación (por ejemplo, MTTR (tiempo medio de remediación), porcentaje de vulnerabilidades críticas parcheadas, reducción de riesgos al aplicar una campaña específica).	Si
	La plataforma debe ofrecer una capa de exposición unificada, que consolide vulnerabilidades, configuraciones inseguras y parches faltantes en una única vista de riesgo por activo y por aplicación.	Si
CARACTERÍSTICAS		
	Actualizar los servidores sin interrumpir el servicio	Sí
	Administración de parches para más de 11.000 aplicaciones de terceros en Windows, Linux y Mac	Si
	La plataforma deberá contar con un dashboard donde se visualice el nivel cumplimiento de los equipos gestionados	Si
	La plataforma debe permitir la creación de políticas de remediación autónomas, capaces de aplicar automáticamente correcciones (parches, scripts, mitigación) basadas en criterios de riesgo predefinidos (por ejemplo, CVE explotados activamente por encima de una determinada puntuación).	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
	Debe presentar la clasificación de riesgo y priorizar las vulnerabilidades a corregir en orden de criticidad no solo desde CVE, sino también en relación al 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 de que se trata cada CVE	Sí

	Actualización en tiempo real de vulnerabilidades	Sí
	Debe admitir al menos el número de vulnerabilidades heredadas igual o superior a 160.000 que se presentan 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 1000 scripts	Sí
	Librería de scripts públicos de múltiples fuentes	Sí
	Protección contra vulnerabilidades del día 0	Sí
	Poseer un módulo de vulnerabilidades integrado para realizar escaneos de vulnerabilidades	Si
	Deberá poder permitir la visibilidad del porcentaje de cumplimiento de compliance según benchmark del NIST mínimamente de sistemas operativos windows y linux	Si
	La solución debe permitir una remediación autónoma de extremo a extremo (desde el descubrimiento hasta la remediación), con una mínima intervención manual, manteniendo al mismo tiempo registros de auditoría completos.	Si
AGENTE		
	Los agentes deben poder como mínimo escanear y parchear al menos los sistemas operativos más comunes: Windows, Linux y Mac	Si
	El agente debe funcionar con un bajo consumo de recursos (CPU, memoria y disco), lo que es adecuado para estaciones de trabajo, servidores y máquinas virtuales en la nube, incluso durante los períodos pico de escaneo y remediación.	Si
	El agente debe poder parchearse a sí mismo.	Si
	El agente debe poder realizar tareas incluso en modo fuera de línea, reenviando los resultados y el estado de la remediación cuando se restablezca la conectividad.	Si

	El agente debe ofrecer paridad funcional entre Windows, Linux y macOS, incluido el descubrimiento, la evaluación, la aplicación de parches y otros métodos de reparación compatibles.	Si
INTEGRACIONES Y REPORTES		
	La plataforma debe soportar integraciones con SIEMs (Splunk, Sumo Logic, etc).	Si
	La solución debe proporcionar webhooks e integraciones basadas en eventos para activar playbooks en herramientas de automatización y SOAR.	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, etc)	Si
	La plataforma debe soportar la integración con herramientas de gestión de incidentes; para la gestión, seguimiento y análisis forense de incidentes de seguridad de forma automatizada.	Si
	Genere informes sobre vulnerabilidades encontradas en uno de los siguientes tipos: formatos PDF con exportación a CSV, PDF: • Resumen ejecutivo, con información resumida sobre el escaneo • 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 los equipos gestionados	Si
	La plataforma debe poder gestionar inventarios de dispositivos	Si

	La plataforma deberá facilitar la gestión de manera centralizada y con visibilidad total de las acciones (actividad, eventos, auditoria)	Si
	Debe contar con integración con herramientas de terceros para hacer Network Scanning (ejemplo Nmap)	Si
	La plataforma ofertada deberá poder realizar un escaneo/evaluación de vulnerabilidades con los siguientes alcances como mínimo: - Network Vulnerability Scan - Full Vulnerability Scan - Authenticated scanning supporting multiple credential types - Compliance scanning CIS	Si
Compliance		
	La plataforma debe permitir el mapeo de los controles de cumplimiento con marcos y estándares (por ejemplo, CIS, ISO 27001, NIST, LGPD), con visualización de la adhesión por política.	Si
	La plataforma debe incluir capacidades para auditoría de cumplimiento basadas en benchmarks CIS o equivalentes, enfocadas en versiones empresariales de sistemas operativos y aplicaciones críticas.	Si
	Debe contar con un Panel de cumplimiento dedicado con visibilidad clara de los resultados de auditoría y trazabilidad de eventos	Si
Carta de autorización del Fabricante		
	Carta de Autorización del Fabricante	Si
Soporte técnico - Requisitos de Formación Técnica del Personal del Oferente		
	Para la correcta instalación configuración y operación de los sistemas ofertados, el oferente deberá contar con mínimo un (1) profesional técnico, que cuente con 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, dichas certificaciones deberán acompañar los currículum de los profesionales técnicos propuestos como parte de la documentación de la oferta.	Si

ITEM 2: Herramienta para detección, respuesta extendida y disminución de superficie de ataque para 500 dispositivos.

N°	Descripción del Requerimiento	Exigido

Protección a estaciones de trabajo y servidores		
	Sistema unificado de prevención, protección, detección avanzada y respuesta, con características extendidas de análisis y correlación de eventos a nivel del dispositivo y otras fuentes adicionales.	Si
	Sistema de identificación de amenazas desconocidas a través de un sandbox	Si
	Análisis integrado de riesgos en los dispositivos y endurecimiento, incluyendo gestión de riesgo de los dispositivos	Si
	Sistema de prevención de ataques de red	Si
	Detección y búsqueda basado en la Nube	Si
	Detección basada en heurística avanzada	Si
	Detección en la etapa pre-ejecución basada en Machine Learning e IA.	Si
	Sistema de prevención de intrusión basado en el host	Si
Administración centralizada de la solución		
	La solución debe disponer de una consola de administración unificada que se administre en la nube (Consola WEB) con capacidad de administrar un número ilimitado de equipos.	Si
	La solución debe proporcionar un único punto para la implementación, aplicación y administración de las políticas de seguridad para el número de puntos finales solicitados por la institución, siendo estos de cualquier tipo y en cualquier ubicación.	
	La solución debe aportar múltiples capas de seguridad para puntos finales, incluyendo servidores de correo de Microsoft Exchange, asegurando protección antimalware con monitorización del comportamiento, protección contra amenazas de día cero, control de aplicaciones y entorno de pruebas, cortafuego, control de dispositivos, control de contenidos, antiphishing y antispam.	

	La solución debe brindar soporte para múltiples plataformas sin importar el número de portátiles, equipos de escritorio y servidores Windows, Linux y Mac OS X, contando con las tecnologías antimalware mejor valoradas. Además, para sistemas Windows debe brindar una seguridad aún más avanzada con un cortafuego bidireccional, detección de intrusiones, control y filtrado de acceso Web, protección de datos sensibles, y control de aplicaciones y de dispositivos. La heurística proactiva de la solución debe clasificar los procesos maliciosos según su comportamiento, asegurando la detección de nuevas amenazas en tiempo real.	
	La solución debe brindar seguridad para centros de datos virtualizados; protegiendo a través de tecnologías de próxima generación que puedan detectar actividades en estado de pre-ejecución, utilizando modelos de Machine Learning especializados y técnicas de análisis del comportamiento entrenados para detectar herramientas de pirateo, exploits y técnicas de ocultación de malware. Bloquea eficazmente los ataques que pasan por alto tanto las defensas tradicionales para dispositivos como las denominadas defensas de última generación en sistemas Windows y Linux.	
	La solución debe incluir un mecanismo automático de detección de redes que le permita detectar otros puntos finales en la red de la institución. Los puntos finales detectados deben mostrarse como puntos finales no administrados en la Consola de Administración.	
	La solución debe permitir instalar los agentes de seguridad en puntos finales físicos y virtuales ejecutando los paquetes de instalación localmente o ejecutando tareas de instalación remotamente desde la Consola de Administración.	
	Adicionalmente la consola de administración, será capaz de gestionar un enlace web (Link de descarga) el cual podrá ser enviado por mail para realizar la instalación remota de clientes fuera de la red corporativa, el mismo se deberá autoconfigurar para enlazarse con la consola web, sin intervención del personal de TI	
	El kit de instalación para los dispositivos debe permitir instalar la protección en dispositivos sin conexión a Internet o con conexiones lentas.	
	Debe utilizar un solo paquete, tanto para sistemas operativos de 32 bits como de 64 bits: • SO Windows: sistemas de 32 bits y 64 bits • SO Linux: sistemas de 32 bits y 64 bits • Mac OS X: solo sistemas de 64 bits	
	La solución debe garantizar que el agente en los equipos administrados ejecute el análisis en tiempo real, incluso cuando no haya conexión, cumpliendo las tareas, políticas y requerimientos configurados previamente aun cuando no haya conexión con la Consola de Administración.	

	El agente de seguridad debe detectar automáticamente la configuración del punto final y adaptar la tecnología de análisis.	
	Debe permitir la visibilidad, administración y consulta de los puntos finales físicos y virtuales, gestionándolos desde la consola de administración. La consola debe permitir la creación ilimitada de grupos o carpetas o subgrupos con el fin de permitir una mejor organización y administración de políticas.	
	La consola debe permitir la asignación de políticas directas a nivel del dispositivo, grupo de dispositivos, unidad de gestión. Además, soportar la asignación basada en reglas como, por ejemplo, por IP, usuario, DNS, puerta de enlace o Gateway, WINS, DHCP, etiqueta.	
	La solución de seguridad debe permitir gestionar en la web a través de una consola alojada en la nube lista y provista en su totalidad por el fabricante (Cloud) desde un único punto de administración a través de cualquier tipo de dispositivo con acceso internet en cualquier sitios del mundo sin límite de usuarios, la consola Web Control Center, facilitará el acceso y la administración de la estrategia general de seguridad, las amenazas a la seguridad global, y el control sobre todos los módulos de seguridad que protegen a los equipos de escritorio virtuales o físicos y a los servidores.	
	Tener capacidad de arquitectura de replicadores y/o servicios de comunicación para gestionar los dispositivos en la red, y proveyendo las siguientes capacidades: - Posibilidad de gestión de ubicaciones remotas a través de uno o múltiples replicadores. El replicador actuará como un servidor proxy de la consola, recopilando y reenviando los datos al servidor principal. - Maneja la comunicación y actualización de los agentes, siendo capaz de manejar centenares de clientes y manteniendo su elevada velocidad operativa sin saturar la infraestructura. - Apoyar la detección de dispositivos no protegidos, a través de un mecanismo automático de detección de red, realizando descubrimiento de todos los equipos de la red que no están protegidos y/o administrados.	
	Configuración de notificaciones vía correo electrónico a partir de eventos.	
	Ejecutar las políticas directamente en el agente y aplicar políticas específicas para los dispositivos incluso cuando no haya conexión con el servidor consola o a través del uso de un usuario con permisos configurados previamente en la política.	
	Recopilar datos necesarios para generar los informes; los registros restantes se deberán almacenar en el cliente para mejorar el rendimiento de la base de datos.	

	Crear múltiples cuentas de usuarios y personalizarlas, los privilegios para cada una se podrán personalizar en forma individual. Se podrá usar en muchas ubicaciones distintas y permitirá definir políticas corporativas para los administradores locales.	
	La herramienta permitirá realizar acciones en caso de ser necesario. Además de mostrar los informes a través de la consola basada en la Web, se pueden exportar en formato PDF, Excel y guardar en una ubicación predefinida, y enviarse como una notificación por correo electrónico.	
	La solución deberá contar con un módulo de protección que proteja las aplicaciones más comunes como: lectores de PDF, navegadores web, clientes de correo, etc en caso de que se trate de explotar una vulnerabilidad.	
	Protección contra vulnerabilidades: Mejora la detección de las Vulnerabilidades y Exposiciones Comunes (CVE) en los protocolos más utilizados, como SMB, RPC y RDP. Brinda protección contra las vulnerabilidades para las cuales aún no se publicó o desarrolló la revisión necesaria.	
	Protección anti botnets: Protege ante las infiltraciones por malware de tipo botnet, previniendo el envío de spam y evitando que se lleven a cabo ataques de red desde los dispositivos.	
	Desinstalación de soluciones de seguridad: la solución deberá ser capaz de desinstalar la solución que se encuentra instalada actualmente de existir.	
	Deberá contar con la posibilidad de sincronizarse con el directorio activo (AD).	
	La consola de gestión debe mostrar la lista de servidores y estaciones que tienen el antivirus instalado, conteniendo la siguiente información mínima: nombre de la máquina, versión de antivirus, versión del motor, fecha de la vacuna, la última fecha de verificación, política aplicada, IP, sistema operativo y el estado.	
	Se deberá poder visualizar el estado de la red desde paneles, portlets o widgets que sean completamente personalizables, tanto en cantidad como en contenido. Dicha información será en tiempo real y se podrá elegir si verla en formato gráfico o tabla	
La solución Dispositivos deberá proteger las siguientes plataformas:		

	La solución deberá brindar prevención, detección y respuesta sobre las plataformas del parque tecnológico de la Convocante que se encuentren dentro del período de soporte oficial de su respectivo fabricante, abarcando como mínimo: • *Estaciones de trabajo y servidores Windows en versiones con soporte vigente de Microsoft.* • *Distribuciones Linux de clase empresarial en versiones con soporte vigente del proveedor, abarcando como mínimo las familias RHEL, Ubuntu LTS, Debian, Fedora, Amazon y SUSE soportadas.* • *macOS en versiones con soporte de seguridad vigente de Apple.* • *Entornos de virtualización, en versiones soportadas por su fabricante, abarcando como mínimo: VMware, Citrix, Red Hat, Oracle, Nutanix.* • *Navegadores. El requisito de compatibilidad con navegadores se limitará a versiones con soporte activo del fabricante, abarcando como mínimo: Mozilla Firefox, Google Chrome, Safari, Microsoft Edge, Opera.*	
Capacidades de detección y Respuesta Extendida		
	La solución deberá proporcionar información detallada de los incidentes detectados, un mapa interactivo de incidentes y acciones correctivas • Detección y visualización de actividades sospechosas • Detección de anomalías • Análisis de causa raíz • Etiquetado de eventos MITRE • Puntuación de confianza respecto a la amenaza • Indicadores de ataque • Shell de comandos remotos • Investigación guiada de incidentes • Opciones avanzadas de contención de amenazas • Análisis de Sandbox • Servicio opcional de detección y respuesta administradas	
	La solución deberá tener estos componentes principales: 1. Un sensor, que recopila y procesa datos para informar datos sobre el punto final y el comportamiento de la aplicación. 2. Security Analytics, un componente utilizado para interpretar los metadatos recopilados por el sensor. 3. Tecnología de correlación de eventos entre terminales conocida como eXtended Endpoint Detection and Response XEDR. Capacidad para detectar ataques avanzados en múltiples puntos finales en infraestructuras híbridas (estaciones de trabajo, servidores o contenedores, ejecutando varios sistemas operativos)	

	Detección posterior al compromiso de actividad sospechosa La solución deberá supervisar los eventos de punto final en busca de signos de ataque y generar un incidente cuando se detecte dicha actividad. 1. Tiene la capacidad de basar los sistemas en función de los indicadores de ataque MITRE y la inteligencia de amenazas de la solución. 2. Cualquier desviación de la línea de base se deberá informar como posible incidente.	
	Investigación de incidentes y visualización 1. La solución proporciona soporte para el análisis de incidentes al proporcionar herramientas para ayudar a filtrar, investigar y tomar medidas en todos los eventos de seguridad detectados por el sensor durante un intervalo de tiempo específico. 2. La solución asigna un valor de puntaje de confianza que indica el grado de certeza de que un evento de seguridad es peligroso. 3. La solución se integra con la base de conocimiento ATT & CK de MITRE y etiqueta los eventos de seguridad de manera adecuada. 4. Los eventos de seguridad se pueden buscar por nombres de archivo, direcciones IP, nombres de host o IOC. También proporciona una función de búsqueda avanzada que permite al usuario pasar por eventos pasados según un criterio complejo. Las consultas predefinidas están diseñadas para casos de búsqueda de eventos de seguridad útiles. 5. La solución proporcionara una visualización sofisticada de eventos de seguridad con información específica o acciones con la siguiente información: a. La pestaña Resumen proporciona una visión general del impacto del evento e información detallada sobre cada nodo de evento. b. La función de línea de tiempo recopila información sobre el desarrollo de eventos de seguridad en un orden cronológico. c. Remediation Actions recopila información sobre las acciones de bloqueo que La solución realiza automáticamente en el evento de seguridad actual. La solución puede bloquear archivos / procesos de la lista usando los valores hash MD5 / SHA256. Puede hacerse desde el incidente de seguridad o importarse desde un archivo CSV.	
Contención de amenazas		

	La solución proporciona las siguientes acciones correctivas para la contención de amenazas. A. Remediación rápida: La solución puede aplicar acciones correctivas desde esta sección como una solución temporal al evento de seguridad. 1. Matar: evita que un proceso se ejecute en el entorno. Esto crea una tarea de proceso de eliminación en el punto final local. Los procesos System32 y de la solución de seguridad están excluidos de esta acción. 2. Archivo de cuarentena: almacena el elemento en cuestión y evita que ejecute su carga útil. 3. Aislar host: La solución aísla el host de la red. El punto final objetivo retiene la comunicación con los servicios de solución de Seguridad B. Acciones de red: La solución proporciona esta solución para la contención de ataques en toda la red 1. Agregar archivo a la lista de bloqueo: el archivo es una pregunta que se puede agregar a una lista de bloqueo y se puede evitar que el ataque se propague lateralmente en la red. 2. Agregar archivo como excepción: para un archivo no malicioso, esta opción se puede usar para excluir actividades legítimas. C. Investigar acciones: La solución aprovecha los componentes internos y las soluciones de terceros para una mayor investigación. 1. Virustotal 2. Sandbox 3. Google D. Conexión remota 1. La solución puede conectarse remotamente al host para investigar rápidamente los ataques, recopilar datos forenses y remediar las infracciones. 2. Elimina la incertidumbre y reduce en gran medida cualquier tiempo de inactividad que resulte de un ataque. 3. Permite que un usuario/administrador autorizado acceda de forma segura a puntos finales administrados directamente desde la consola. 4. Después de conectarse con éxito al punto final remoto, se pueden ejecutar varios comandos de shell personalizados directamente en el sistema operativo para remediar la amenaza al instante o recopilar datos para una mayor investigación. Además de los casos de uso anteriores, el módulo también proporciona visualización de los eventos de seguridad que están bloqueados por las capas preventivas. E. Defensa contra ataques sin archivos: Detecte y bloquee malware basado en scripts, sin archivos, ofuscado y personalizado, con reparación automática. F. Capacidades de prevención avanzadas como PowerShell Defense, Exploit Defense y detección de anomalías, bloqueo de ataques al principio de la cadena de ataque, antes de la ejecución	
Protección en tiempo real		

	El análisis de la solución en tiempo real debe evitar que entren en el sistema nuevas amenazas de malware, La solución debe analizar los archivos locales y de red cuando se acceda a ellos (al abrirlos, moverlos, copiarlos o ejecutarlos), al análisis de los sectores de arranque y al de las aplicaciones potencialmente no deseadas (APND).	
Filtrado de correo electrónico malicioso.		
	El módulo de protección de correo electrónico de la solución debe ofrecer protección multicapa contra las amenazas y phishing mediante una combinación de varios filtros y motores de análisis en la capa de protocolo (POP3 y SMTP) para determinar si los mensajes de correo electrónico son maliciosos.	
Filtrado de Navegación		
	La solución que controla el tráfico HTTP / FTP del Explorador de Windows debe permitir o denegar el tráfico HTTP y FTP desde el Explorador de Windows. La solución debe tener la capacidad de crear reglas de cortafuego adicionales para otras aplicaciones instaladas en los puntos finales, esto debe crearlo además de las reglas predeterminadas por defecto.	
Remote Troubleshooting		
	La solución debe permitir recopilar registros básicos y avanzados de forma remota. Esto con el fin de facilitar el análisis en profundidad de problemas y proporcionar una resolución más rápida.	
Protección Proactiva		
	La solución debe poseer tecnología de detección proactiva e innovadora que debe utilizar avanzados métodos heurísticos para que pueda detectar nuevas amenazas potenciales en tiempo real, debe monitorizar continuamente las aplicaciones que se están ejecutando en el punto final en busca de acciones indicativas de malware. Cada una de estas acciones deben puntuarse y calcular una puntuación global para cada proceso.	
Consumo de recursos de memoria del endpoint		
	La solución debe utilizar recursos mínimos (>~220MB) cuando se ejecute un análisis completo	
Exclusión de archivos del análisis en tiempo real		
	La solución deberá contar con la opción para realizar exclusiones de archivos del análisis en tiempo real.	

Control de acceso web		
	La suite de seguridad deberá contar con un control de acceso web, con categorías para definir qué sitios pueden ser accedidos o no dentro de la red. Limitar el acceso a los sitios web por categoría y por grupo de usuarios para lograr una eficaz aplicación de las políticas corporativas cuyo objetivo es maximizar el cumplimiento de directivas de seguridad y la productividad de los empleados.	
Análisis manual de búsqueda de códigos maliciosos.		
	La solución deberá contar con la opción de correr un análisis manual de búsqueda de códigos maliciosos. Ofrecer detección avanzada de malware furtivo mediante la exploración minuciosa del contenido de los protocolos seguros HTTPS y POP3S, así como de los archivos comprimidos.	
ERM (Administración de Riesgos)		
	El módulo de gestión de riesgos de punto final (ERM) ayudará a identificar y remediar una gran cantidad de riesgos de red y sistemas operativos a nivel de punto final, mostrando el porcentaje de vulnerabilidad en la infraestructura. El puntaje de riesgo de la compañía se calcula teniendo en cuenta una amplia lista de indicadores de riesgos y vulnerabilidades de aplicaciones conocidas, mostrando su evolución en el tiempo. Desglose de la puntuación y las principales configuraciones incorrectas y los widgets de aplicaciones vulnerables hacen que sea más fácil ver dónde su entorno es más vulnerable a los ataques y qué dispositivos son los más afectados. Este módulo deberá contar con al menos 300 indicadores de gestión de Hardening para la generación del nivel de riesgo.	
Human Risks Analytics		

	El módulo de gestión de riesgos debe incluir un analizador de riesgos humanos. El cual debe validar los siguientes aspectos: · Verificar si el usuario ha enviado credenciales a través de conexiones HTTP inseguras desde el último escaneo. · Verificar si el usuario ha navegado o no sitios marcados como phishing o fraude desde el último análisis. · Verificar si el usuario ha estado expuesto a una gran cantidad de amenazas desde el último análisis. · Verificar si el usuario ha estado expuesto a una amenaza de un dispositivo extraíble (por ejemplo, unidad flash, disco duro externo) desde el último escaneo. · Verificar si el usuario ha accedido a archivos maliciosos a través de una carpeta compartida de red desde el último análisis. · Verificar si el usuario ha accedido a alguna URL maliciosa desde el último análisis. · Verificar si el usuario no ha cambiado la contraseña de inicio de sesión de la cuenta (local o de dominio) durante más de 30 días. · Verificar si el usuario usa las mismas contraseñas en diferentes sitios externos. · Verificar si el usuario usa las mismas contraseñas compartidas entre sitios web internos y externos. Verificar si el usuario no ha cambiado la contraseña de inicio de sesión para las cuentas HTTP (internas o externas) durante más de 30 días.	
Defensa de ataques de RED		
	Tecnología enfocada en detectar técnicas de ataque a la red diseñadas para obtener Acceso a puntos finales específicos como: • Ataques de fuerza bruta • Ataques de red • Ladrones de contraseñas • Ataques Laterales	
Anti-Exploit Avanzado		
	Anti-Exploit proporciona protección en ejecución contra intentos de explotación dirigidos a vulnerabilidades conocidas y desconocidas en aplicaciones de uso común y aplicaciones propias, como el navegador, Microsoft Office o Adobe Reader, así como contra intentos específicos de post-explotación en modo kernel.	
Control de Dispositivos		

	Control de Dispositivos: permite prevenir las infecciones de fugas y malware de datos sensibles a través de dispositivos externos conectados a extremos aplicando bloqueo normas y excepciones a través de la política a una amplia gama de tipos de dispositivos (tales como unidades Flash USB, dispositivos Bluetooth, reproductores de CD/DVD, dispositivos de almacenamiento, etc.). Que los bloqueos a dispositivos puedan realizarse por marca, modelo, número de serie o usuario.	
Cifrado de Disco (Opcional)		
	La solución debe contar con la opción de adicionar como Add-on la protección de los datos de toda la unidad de disco duro del dispositivo aprovechando los mecanismos de cifrado proporcionados por Windows (BitLocker) y Mac (FileVault). Se basa en el cifrado nativo de los dispositivos para garantizar la total compatibilidad y maximizar el rendimiento, sin la necesidad de instalar un agente adicional, ni un servidor de claves, gestionado todo de la misma consola de administración. Debe poseer opción para establecer reglas para excluir unidades del cifrado.	
Análisis Programados		
	La solución y la consola de administración remota deberán permitir realizar análisis programados de los discos duros locales. Esta programación se podrá configurar en forma diaria, semanal, mensual.	
Cortafuegos de escritorio		
	La solución deberá contar con un cortafuego de escritorio (Firewall Personal) que cuenta con un filtrado dinámico de paquetes que provea de monitoreo y filtrado de tráfico de Red, y tenga total protección para IPv4 e IPv6 y con la opción de agregar reglas y servicios al cortafuego en forma autónoma y centralizada. Impedir el acceso no autorizado a la red corporativa. Ofrecer una fácil instalación, gran capacidad de personalización de reglas y un modo de aprendizaje inteligente para crear reglas de firewall automáticamente basándose en el tráfico de red observado. Combinar perfiles personalizados de firewall con zonas de redes de confianza. Debe poseer distintos modos del módulo de firewall entre los cuales debe tener uno que permita aprender la conducta del usuario generando las reglas permisivas automáticamente. Debe poseer opción para importar y exportar reglas. Esta solución no deberá provocar interrupciones con el Firewall de la Institución.	
	La solución debe forzar el endurecimiento dinámico y personalizado que previene ataques Living-off-the-land (LOTL) sin impactar la productividad ni sobrecargar equipos de TI.	

	La solución debe integrarse perfectamente en las arquitecturas existentes dentro de plataformas XDR, proporcionando visibilidad, priorización y mitigación de riesgos de 360°.	
	La solución debe ofrecer endurecimiento personalizado mediante el aprendizaje del comportamiento de los usuarios y la restricción segura de herramientas innecesarias y peligrosas para determinados usuarios.	
	La solución debe proporcionar reducción dinámica de la superficie de ataque, adaptándose de forma continua y autónoma a cambios en el comportamiento de usuarios y nuevos vectores de amenazas, minimizando el esfuerzo administrativo.	
	La solución debe facilitar control preciso, aplicando restricciones en aplicaciones que no se utilizan y son peligrosas, así como restricciones a nivel de acciones dentro de aplicaciones utilizadas, bloqueando solo comportamientos atípicos.	
	La solución debe integrar protección basada en inteligencia sobre amenazas, garantizando eficiencia contra los últimos vectores de amenazas. La solución debe incluir una agrupación inteligente de usuarios con comportamientos similares para un endurecimiento eficiente en toda la organización.	
	La solución debe ofrecer mitigación autónoma de riesgos con modo automático para cambios adaptativos sin intervención, y modo manual para recomendaciones que requieren decisiones del administrador.	
	La solución debe bloquear anticipadamente ataques LOTL restringiendo acceso a herramientas como PowerShell o WMI.	
	La solución debe reducir drásticamente la superficie de ataque, deteniendo ataques sigilosos antes de causar daños, abordando técnicas LOTL usadas en el 70% de los ataques.	
	La solución debe ser compatible con funcionalidades como inspección profunda de procesos y razonamiento avanzado.	
	Actualización a través de repositorios de actualización de la solución de todas las estaciones protegidas	
	La consola de administración deberá permitir actualizar a través de repositorios de actualización a todas las estaciones protegidas con la posibilidad de tener redundancia de repositorios de actualización en forma automática (Fail-over).	

	Las actualizaciones de las bases de datos de firmas de códigos maliciosos deberán ser incrementales, evitando de esta manera la saturación del ancho de banda en su despliegue.	
	Análisis de archivo comprimidos	
	La solución ofertada deberá detectar virus en archivos compactados, con profundidad máxima (16), en los siguientes formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y otros	
Gestión de Políticas		
	La consola de administración deberá definir y hacer cumplir consistentemente las políticas a lo largo de la red. El Administrador de Políticas facilitará la importación/exportación, para permitir la aplicación y combinación de las políticas de diversas maneras.	
Certificaciones		
	La solución deberá contar con certificaciones para trabajar en ambientes virtuales como VMWare, Citrix y Nutanix.	
Soporte Técnico		
	El oferente estará obligado a prestar el servicio de soporte y resolución de problemas o incidentes en los sitios de instalación de la herramienta cuando el problema lo amerite.	
	El oferente deberá asignar como mínimo a un técnico certificado que acudirá a las oficinas del contratante para la instalación de la solución.	
	El soporte técnico estará vigente durante el periodo de licenciamiento	
Capacitación		
	El oferente deberá capacitar a hasta 5 (cinco) funcionarios técnicos de la entidad contratante en el manejo de la solución y de las nuevas versiones que puedan generarse durante el tiempo que dure el licenciamiento.	

	El oferente deberá contar con un responsable directo del fabricante, el mismo que deberá efectuar visitas periódicas para de esta manera poder informar sobre el seguimiento en la parte de atención al cliente en lo comercial y en lo técnico por parte del oferente.	
Carta de autorización del Fabricante		
	Carta de Autorización del Fabricante	Si
Soporte Técnico - Certificaciones Técnicas mínimas del Fabricante		
	El fabricante debe poseer certificaciones internacionales, incluyendo SOC2 Type 2 Compliant, ISO 27001, ISO 9001. La solución propuesta deberá estar posicionada en los cuadrantes de liderazgo de los principales análisis de mercado independientes, específicamente Gartner (Magic Quadrant for Endpoint Protection Platforms) y Forrester. Los proponentes deberán demostrar capacidades efectivas en detección y respuesta (EDR/XDR) mediante resultados consistentes y públicos en las evaluaciones de MITRE ATT&CK Evaluations, demostrando altos niveles de visibilidad y detección sin configuración previa. El fabricante debe poseer su propio centro de investigación y desarrollo (laboratorio) para la investigación y desarrollo de modelos de detección de actividades maliciosas.	

ITEM 3: Herramienta para Gestión de Eventos, implementación como Solución de Seguridad.

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
	La plataforma debe contar con APIs completas y bien documentadas que permitan integraciones, automatización de procesos y consumo de datos por herramientas externas.	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
	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
	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 inventario de activos mediante la recolección de información de endpoints, incluyendo sistema operativo, hardware, interfaces de red y software instalado, lo que permite mantener una visibilidad actualizada de los activos de TI.	Si
	La plataforma debe ser capaz de operar en entornos aislados (air-gapped) o con conectividad restringida, incluyendo mecanismos para actualizaciones offline y sincronización de inteligencia de amenazas.	Si
Carta de autorización del Fabricante		

	Carta de Autorización del Fabricante	Si
Soporte técnico - Requisitos de Formación Técnica del Personal del Oferente		
	Para la correcta instalación configuración y operación de los sistemas ofertados, el oferente deberá contar con mínimo un (1) profesional técnico, que cuente con 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, dichas certificaciones deberán acompañar los currículum de los profesionales técnicos propuestos como parte de la documentación de la oferta.	Si

ITEM 4: Diseño, implementación y operación asistida de Centro de Operaciones de Seguridad por 24 meses

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 robustos 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
	Recomendar 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
	Recomendar 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		
	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 y 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
	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

<table>
<tr>
<td></td>
<td>
Cumplir con métricas de desempeño alineadas con estándares internacionales en sus últimas versiones vigentes, como NIST SP 800-61 Rev. 3, ISO/IEC 27001:2022 e ISO/IEC 27035 (partes 1, 2 y 3 en sus ediciones vigentes).
<table>
<tr><th>KPI</th><th>Nombre Completo</th><th>Objetivo</th></tr>
<tr><td>MTTD</td><td>Mean Time to Detect</td><td>< 4 horas (Critical/High) < 1 hora con XDR + IA</td></tr>
<tr><td>MTTR</td><td>Mean Time to Respond</td><td>< 4 horas (P1/Critical) < 2 horas (High)</td></tr>
<tr><td>MTTC</td><td>Mean Time to Contain</td><td>< 4 hora (Critical) < 2 horas (High)</td></tr>
<tr><td>MTTA</td><td>Mean Time to Acknowledge</td><td>< 4530 minutos</td></tr>
</table>
<table>
<tr><th>KPI</th><th>Nombre Completo</th><th>Objetivo Recomendado</th></tr>
<tr><td>FPR</td><td>False Positive Rate</td><td>< 20% general < 15% con tuning + IA</td></tr>
<tr><td>MITRE ATT&CK Coverage</td><td>MITRE ATT&CK Coverage</td><td>≥ 70% de tácticas críticas 100% cobertura eventual</td></tr>
<tr><td>DEDUP</td><td>Auto-Deduplication Rate</td><td>> 90%</td></tr>
<tr><td>ESC L1→L2</td><td>Tiempo Escalada L1 → L2</td><td>< 45 minutos (Critical/High)</td></tr>
<tr><td>POST-M</td><td>Post-Mortem Rate</td><td>> 90% de casos cerrados con lecciones aprendidas</td></tr>
</table>
</td>
<td>Si</td>
</tr>
<tr>
<td></td>
<td>Establecer un proceso de gestión de evidencias forenses para investigaciones de incidentes, asegurando la cadena de custodia y cumplimiento legal.</td>
<td>Si</td>
</tr>
</table>

	Implementar un sistema de retroalimentación para mejorar procesos del SOC, basado en lecciones aprendidas de incidentes y simulacros.	Si
Alcance Detallado		
	Monitorear aproximadamente 500 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
a. 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 500 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 haran en concordancia con el personal de TI de la CONATEL. La empresa adjudicada debe brindar el acompañamiento necesario.	Si
Indicadores de cumplimiento:		
	Informe de pruebas de penetración entregado dentro de los 30 días hábiles posteriores a la finalización de las pruebas.	Si
	Recomendación de mitigación de vulnerabilidades críticas y altas dentro de los 90 días corridos establecidos, que no requieren inversión económica.	Si
	Evidencia de pruebas de verificación post-remediación para confirmar la resolución de vulnerabilidades	Si

ITEM 5: Diseño e Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI-TI)

N°	Descripción del Requerimiento	Exigido
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.	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, 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 de la CONATEL	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, 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

	Suscribirse a cursos especializados en español para 5 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
b. 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.	Si
	Desarrollar un plan de auditoría que cubra los 4 dominios de ISO 27001, priorizando controles críticos como - Políticas para la seguridad de la información -Definición de roles y responsabilidades de seguridad y Gestión de accesos privilegiados	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 del área de IT.	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

Detalle de los bienes y/o servicios

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

Ítem	Descripcion	Unidad de medida	Cantidad	ESPECIFICACIONES TECNICAS Y NORMAS

	Herramienta para monitoreo y remediación de vulnerabilidades para 500 dispositivos	**Unidad**	**1**	Implementación de una **PLATAFORMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)**, así como también, un centro de operaciones de ciberseguridad, por sus siglas en inglés **SOC** (Security Operations Center), con base en el Centro de Datos ubicado en **la** institución, **CONATEL**, enfocado principalmente en la infraestructura crítica definida en el proyecto, incluyendo Redes corporativas y dispositivos de usuario final
	Herramienta para detección, respuesta extendida y disminución de superficie de ataque para 500 dispositivos	**Unidad**	**1**	
	Herramienta para Gestión de Eventos, implementación como Solución de Seguridad para 500 activos	**Unidad**	**1**	
	Diseño, implementación y operación asistida de Centro de Operaciones de Seguridad	**Mes**	**24**	
	Diseño e Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI-TI)	**Unidad**	**1**	

De las MIPYMES

En los 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:

Ítem	Descripción del bien	Cantidad	Unidad de medida de los bienes	LUGAR DE ENTREGA DE LOS BIENES	FECHAS FINALES DE ENTREGA DE LOS BIENES
1.	Herramienta para monitoreo y remediación de vulnerabilidades para 500 dispositivos.	1	Unidad	Pte. Franco y Ayolas Edificio AYFRA CONATEL	90 días desde la emisión de la Orden de compra y/o servicio
2.	Herramienta para detección, respuesta extendida y disminución de superficie de ataque para 500 dispositivos	1	Unidad		90 días desde la emisión de la Orden de compra y/o servicio
3.	Herramienta para Gestión de Eventos, implementación como Solución de Seguridad para 500 activos.	1	Unidad		90 días desde la emisión de la Orden de compra y/o 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.

Ítem	Descripción del bien	Cantidad	Unidad de medida de los servicios	Lugar donde los servicios serán prestados	Plazo de ejecución de los servicios
4	Diseño, implementación y operación asistida de Centro de Operaciones de Seguridad	24	Mes	Pte. Franco y Ayolas - Edificio AYFRA CONATEL	24 (veinte y cuatro) meses desde la emisión de la Orden de servicio y/o compra
5	Diseño e Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI-TI)	1	Unidad		180 días desde la emisión de la Orden de compra y/o servicio

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

1. El Proveedor embalará los bienes en la forma necesaria para impedir que se dañen o deterioren durante el transporte al lugar de destino final indicado en el contrato. El embalaje deberá ser adecuado para resistir, sin limitaciones, su manipulación brusca y descuidada, su exposición a temperaturas extremas, la sal y las precipitaciones, y su almacenamiento en espacios abiertos. En el tamaño y peso de los embalajes se tendrá en cuenta, cuando corresponda, la lejanía del lugar de destino final de los bienes y la carencia de equipo pesado de carga y descarga en todos los puntos en que los bienes deban transbordarse.

2. El embalaje, las identificaciones y los documentos que se coloquen dentro y fuera de los bultos deberán cumplir estrictamente con los requisitos especiales que se hayan estipulado expresamente en el contrato y cualquier otro requisito si lo hubiere, especificado en las condiciones contractuales.

Inspecciones y pruebas

Las inspecciones y pruebas serán como se indica a continuación:

No Aplica

1. El proveedor realizará todas las pruebas y/o inspecciones de los Bienes, por su cuenta y sin costo alguno para la contratante.

2. Las inspecciones y pruebas podrán realizarse en las instalaciones del Proveedor o de sus subcontratistas, en el lugar de entrega y/o en el lugar de destino final de entrega de los bienes, o en otro lugar indicado en este apartado.

Cuando dichas inspecciones o pruebas sean realizadas en recintos del Proveedor o de sus subcontratistas se le proporcionarán a los inspectores todas las facilidades y asistencia razonables, incluso el acceso a los planos y datos sobre producción, sin cargo alguno para la Contratante.

3. La Contratante o su representante designado tendrá derecho a presenciar las pruebas y/o inspecciones mencionadas en la cláusula anterior, siempre y cuando éste asuma todos los costos y gastos que ocasione su participación, incluyendo gastos de viaje, alojamiento y alimentación.

4. Cuando el proveedor esté listo para realizar dichas pruebas e inspecciones, notificará oportunamente a la contratante indicándole el lugar y la hora. El proveedor obtendrá de una tercera parte, si corresponde, o del fabricante cualquier permiso o consentimiento necesario para permitir a la contratante o a su representante designado presenciar las pruebas o inspecciones.

5. La Contratante podrá requerirle al proveedor que realice algunas pruebas y/o inspecciones que no están requeridas en el contrato, pero que considere necesarias para verificar que las características y funcionamiento de los bienes cumplan con los códigos de las especificaciones técnicas y normas establecidas en el contrato. Los costos adicionales razonables que incurra el Proveedor por dichas pruebas e inspecciones serán sumados al precio del contrato, en cuyo caso la contratante deberá justificar a través de un dictamen fundado en el interés público comprometido. Asimismo, si dichas pruebas y/o inspecciones impidieran el avance de la fabricación y/o el desempeño de otras obligaciones del proveedor bajo el Contrato, deberán realizarse los ajustes correspondientes a las Fechas de Entrega y de Cumplimiento y de las otras obligaciones afectadas.

6. El proveedor presentará a la contratante un informe de los resultados de dichas pruebas y/o inspecciones.

7. La contratante podrá rechazar algunos de los bienes o componentes de ellos que no pasen las pruebas o inspecciones o que no se ajusten a las especificaciones. El proveedor tendrá que rectificar o reemplazar dichos bienes o componentes rechazados o hacer las modificaciones necesarias para cumplir con las especificaciones sin ningún costo para la contratante. Asimismo, tendrá que repetir las pruebas o inspecciones, sin ningún costo para la contratante, una vez que notifique a la contratante.

8. El proveedor acepta que ni la realización de pruebas o inspecciones de los bienes o de parte de ellos, ni la presencia de la contratante o de su representante, ni la emisión de informes, lo eximirán de las garantías u otras obligaciones en virtud del contrato.

CONDICIONES CONTRACTUALES

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

Interpretación

1. Si el contexto así lo requiere, el singular significa 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.

Formalización de la Contratación

La convocante formalizará la contratación mediante: Contrato.

Documentación electrónica

Cuando las documentaciones se expidan de manera electrónica en cumplimiento de la Ley N° 6715 “DE PROCEDIMIENTOS ADMINSITRATIVOS” 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.

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.
- 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 especificados en el apartado precedente.
- 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.

En caso de consorcio en formación, el mismo deberá actualizar el RUC definitivo del consorcio constituido a través del Registro de Proveedores del Estado, previo a la comunicación del contrato y emisión del código de contratación.

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

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.

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.

Cuando dicha información incluya datos personales de personas físicas, las partes se obligan a realizar su tratamiento en estricto cumplimiento de la Ley N° 7593/2025 “De Protección de Datos Personales”, su reglamentación y demás normas aplicables, respetando en particular los principios de licitud, finalidad, minimización, confidencialidad, seguridad y diligencia debida, y limitando el tratamiento exclusivamente a los fines vinculados con la ejecución del contrato.

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.

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.

Condiciones especiales de la Garantía de Fiel Cumplimiento de Contrato

Las condiciones especiales de la Garantía de Fiel Cumplimiento de Contrato serán:

No Aplica

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 suscripción del contrato hasta el 28 de febrero de 2029.

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 corridos contados a partir de la fecha de cumplimiento de las obligaciones, incluyendo cualquier obligación relativa a la garantía de los bienes y/o servicios.

Solicitud de Pago de Anticipo

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

La solicitud de pago en concepto de Anticipo Financiero equivalente al 20% del monto total ofertado de los Items 1,2 y 3, deberá presentarse dentro de los 10 (diez) dias posteriores a la firma del Contrato, junto con la Garantía de fiel Cumplimiento de Contrato, el mismo deberá ser entregado en la Oficina de la Gerencia Operativa de Contrataciones - Departamento de Contratos, Piso 3 del Edificio Ayfra, sito Pdte. Franco 780 esq. Ayolas en horario de oficina (07:30 a 15:30hs), el mismo debe ser entregado al Abg. Javier Gonzalez (Jefe del Departamento de Contratos) y/o a la Abg. Luz Gomez (Jefa de la Unidad de Gestion de Contratos)- La Garantía de Anticipo Financiero deberá cubrir desde la suscripción del contrato hasta el 28 de febrero de 2029 . El pago del anticipo debera realizarse dentro de los 30 (treinta) dias posteriores a la presentacion de la solicitud por parte del Oferente.

1. El anticipo es la suma de dinero que se entrega al proveedor, consultor o contratista destinada al financiamiento de los costos en que éste debe incurrir para iniciar la ejecución del objeto contractual. El mismo no constituye un pago por adelantado; debe estar amparado con una garantía correspondiente al cien por ciento de su valor y deberá ser amortizado durante la ejecución del contrato y durante la ejecución de contrato demostrar el debido uso. La Garantía de Anticipo deberá estar vigente desde la solicitud de pago del anticipo, y mantener su vigencia hasta su total amortización.

Los recursos entregados en calidad de anticipo no podrán destinarse a fines distintos a los relacionados con el objeto del contrato.

El proveedor, consultor o contratista que reciba pagos en concepto de anticipo estará obligado a informar a la contratante sobre el destino y la forma de aplicación del mismo, que en todos los casos estará relacionado al efectivo cumplimiento del contrato.

En caso de extensión de la Garantía de Anticipo, la misma deberá cubrir el saldo pendiente de amortización.

2. Si se establece en el SICP el otorgamiento de anticipos, no podrá superar en ningún caso el porcentaje establecido en la legislación vigente.

3. La solicitud de pago del anticipo deberá ser presentada por escrito, con la factura, el plan de inversiones y la Garantía de Anticipo.

4. El proveedor podrá remitir una comunicación por escrito a la contratante, en la cual informe que rechaza el anticipo previsto en el PBC. La falta de solicitud de anticipo en el plazo previsto en el PBC será considerada como un rechazo del mismo. En estos casos podrá darse inicio al cómputo de la ejecución contractual en las condiciones establecidas en el pliego de bases y condiciones.

5. El Pago del Anticipo debe ser total. En el caso que se realizare el pago de un porcentaje inferior al 100% del mismo, el proveedor podrá rechazarlo en el plazo de cinco (5) días hábiles mediante una nota de reclamo remitida a la Contratante. Transcurrido dicho plazo, se considerará que el Anticipo ha sido aceptado por el proveedor y podrá darse inicio al cronograma de ejecución contractual en las condiciones establecidas en el pliego de bases y condiciones.

6. En el caso de que el proveedor haya solicitado el anticipo en las condiciones establecidas en la presente clausula y la convocante no ha procedido al pago, el oferente no está obligado a iniciar la ejecución del contrato hasta tanto el pago se haya efectuado de forma total o de acuerdo a lo dispuesto en el punto 5.

7. El proveedor deberá usar el anticipo únicamente para pagar costos que se requieran específicamente para la ejecución del contrato respectivo. El proveedor deberá informar a la contratante sobre el destino y la forma de aplicación del mismo y demostrar que ha utilizado el anticipo para gastos relacionados al efectivo cumplimiento del contrato mediante la presentación de copias de las facturas u otros documentos al administrador del contrato, quien junto con la contratante realizará el seguimiento y control de los recursos entregados. El proveedor estará obligado a proporcionar a la contratante los comprobantes y cualquier otra información que le fuera requerida con el objeto de comprobar el cumplimiento del plan de inversión del anticipo.

8. La amortización del anticipo se realizará de acuerdo con lo establecido en el contrato, en la proporción que éste indique.

9. Para la ejecución de esta garantía, especialmente cuando sea instrumentada a través de Póliza de Seguro de caución, será requisito que previamente el proveedor sea notificado del incumplimiento y la intimación de que se hará efectiva la ejecución del monto asegurado.

10. A menos que se indique otra cosa en este apartado, la Garantía de Anticipo será liberada por la contratante y devuelta al proveedor, a requerimiento de parte, a más tardar treinta (30) días contados a partir de la fecha de cumplimiento de las obligaciones del proveedor en virtud del contrato, pudiendo ajustarse por el saldo adeudado.

11. En el caso de rescisión o terminación anticipada del contrato, los proveedores o contratistas deberán reintegrar a la contratante el saldo por amortizar.

Forma de Instrumentación de Garantía de anticipo

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

póliza de seguro

Disponibilidad de créditos presupuestarios

El alcance de los compromisos asumidos, así como la provisión de los bienes y servicios acordados, quedarán supeditados durante su ejecución, a la efectiva disponibilidad de los créditos presupuestarios y de los planes financieros aprobados para el Ejercicio Fiscal vigente y en los ejercicios fiscales siguientes.

La Entidad contratante debe comunicar formalmente al proveedor la existencia del CDP correspondiente al ejercicio fiscal vigente.

En ausencia del CDP y de su comunicación expresa al proveedor, este quedará eximido de realizar la provisión de bienes y/o servicios, sin que dicha abstención genere responsabilidad alguna ni constituya causal de incumplimiento contractual, aun cuando se hubiera emitido la orden de ejecución.

En ningún caso serán admitidas como deudas del ejercicio fiscal vigente ni dará derecho a reclamación de pago alguno, la

provisión de bienes o prestaciones de servicios que se efectuaren sin contar con la disponibilidad de los créditos presupuestarios correspondientes.

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 *(se indica la fecha que debe presentar según el PBC)*
Orden de Servicio y/o Compra emitida por el Administrador del Contrato para los Items 1-2-3	*Orden de Servicio y/o compra*	*5 (cinco) días hábiles posteriores a la firma del Contrato*
Acta de Conformidad emitida por el Administrador de Contrato para los Items 1-2-3	*Acta de Conformidad*	*Conforme al Plan de entrega de los bienes.*
Orden de Servicio y/o compra emitida por el Administrador del Contrato Item 4	*Orden de Servicio y/o compra*	*Conforme al Plan de Prestación de Servicios*
Acta de Conformidad Mensual emitida por el Administrador de Contrato	*Acta de Conformidad Mensual*	
Orden de Servicio y/o compra emitida por el Administrador del Contrato Item 5	*Orden de Servicio y/o compra*	*Conforme al Plan de Prestación de Servicios*
Acta de Conformidad emitida por el Administrador de Contrato	*Acta de Conformidad*	

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 Nº 7021/22, pudiendo requerir al proveedor o contratista, la información que sea necesaria

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 previsional. En el caso de que no lo hiciera, se considerará incumplimiento del contrato por causa imputable al proveedor o contratista.

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

2.Documentos Específicos a la presente convocatoria:

- El reporte de la carga de la nómina del personal en el FIP, asignado a los servicios contratados o la actualización en su caso;
- La Declaración Jurada del Salario expedida por el Instituto de Previsión Social a fin de corroborar el cumplimiento efectivo de las cargas sociales;
- El extracto de las acreditaciones de pago de salarios al personal asignado, realizadas a través de Red Bancaria;
- Planilla de marcación de entrada y salida de los empleados de la empresa a la institución contratante.

Otras formas y condiciones de pago al proveedor en virtud del contrato serán las siguientes: El pago se realizará contra entrega de los bienes (Items 1-2-3) restado del anticipo financiero (20%). Por el diseño, implementación y operación del Centro de Operaciones de Seguridad de manera mensual (Item 4) y por el diseño e implementación de un Sistema de Gestion de Seguridad de la Informacion contra prestación del servicio (Item 5). La Garantía de Fiel Cumplimiento del Contrato debe ser equivalente al 10% del monto total del Contrato, con vigencia desde la suscripción del contrato hasta el 28 de febrero de 2029.. La contratación es con ejecución plurianual. Para el Ejercicio Fiscal 2027 y 2028 quedara sujeta a la aprobación de la partida presupuestaria respectiva. Para cada pago el Proveedor deberá presentar la solicitud de pago por escrito en la Mesa de Entrada de CONATEL, sito en Presidente Franco 780 entre O´Leary y Ayolas, Edificio Ayfra, indicando el número de factura y número de contrato, adjuntando la factura, documentos que correspondan según el caso (Informes mensuales e Informe final). El Control de los saldos es responsabilidad del Administrador del Contrato y Contratista, ajustándose a la disponibilidad presupuestaria asignada. El Proveedor deberá tener en cuenta lo solicitado para la implementación del Sistema Integrado de Facturación electrónica Nacional (SIFEN), y el Registro de Proveedores en la CONATEL a través de transferencia Interbancaria. El adjudicatario, que se encuentre registrado como FACTURADOR ELECTRÓNICO ante la Administración Tributaria, deberá remitir a la CONATEL, los documentos tributario electrónicos a la siguiente dirección de correo: pagosproveedores@conatel.gov.py. Así también, para solicitar el pago de las obligaciones deberá presentar copia impresa de la factura electrónica acompañado de los 1. Documentos Genéricos ()

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.

Anticipo MIPYMES

Se otorgará Anticipo MIPYMES:

No Aplica

Reajuste

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

Los precios ofertados y adjudicados, estarán sujetos a reajuste de precios, siempre y cuando exista una variación sustancial de precios en la economía nacional y ésta se vea reflejada en el Índice de Precios de Consumo (IPC) publicado por el Banco Central del Paraguay. El reajuste de los precios se realizará conforme a la siguiente fórmula: Pr = P x (IPC1/ 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 de Paraguay, correspondiente al mes de la apertura de ofertas. Los reajustes deberán ser solicitados por escrito a CONATEL por el Proveedor. La solicitud debe realizarse indefectiblemente dentro del mes siguiente al cual se produjeron las variaciones. No se reconocerán reajuste de precios si los bienes/servicios se encuentran atrasados respecto al cronograma de entrega. El reajuste tendrá aplicación sobre los bienes/servicios entregados posteriores al mes en el cual se produjeron las variaciones, previa Resolución de la máxima autoridad del CONATEL

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, cuando la variación sea positiva, para cuya obtención se deberá cumplir con los requerimientos establecidos por la DNCP.

La aplicación de la formula deberá prever la deducción del anticipo financiero, en caso de haber sido otorgado. En caso que los índices oficiales que se deben utilizar en el cálculo no estén disponibles, se podrán efectuar ajustes provisionales utilizando los últimos índices conocidos. Los ajustes se corregirán cuando se conozcan los valores relativos a los meses en cuestión.

El coeficiente de ajuste se redondea a la millonésima superior.

El pago del reajuste se efectuará únicamente después de la emisión del acto administrativo que autoriza el precio reajustado y del correspondiente código de contratación.

Los reajustes de precios se aplicarán bajo solicitud expresa por parte del proveedor, conforme a la forma y plazo establecida en la normativa. El Administrador del Contrato es responsable de velar por la aplicación del reajuste de precios en caso de ser favorable a la Contratante.

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 plazo de 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 correspondientes, 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 solicitar la suspensión del contrato, por motivos que no le serán imputables, de acuerdo a lo establecido en el artículo 66 de la Ley N° 7021/22.

La contratante, en virtud de causas establecidas en el contrato, está facultada para suspender la tramitación de un pago, en tal caso, las sumas correspondientes durante los atrasos resultantes no devengarán intereses por mora.

Pago de interés por mora.

Procedimiento para el pago de interés por mora:

El contratista realizará la solicitud de cobro dentro de los 5 (cinco) días hábiles posteriores al cobro del monto de la factura que incurriere en mora. Se deberá ingresar una nota dirigida a la Gerencia Administrativa Financiera adjuntando los datos principales de la factura (número, fecha de emisión, monto y los datos de este proceso vinculado a la misma), comprobante de transferencia bancaria o cheque que acredite la fecha de recepción de los fondos y la planilla de liquidación, la cual consta de la siguiente fórmula: I = Monto neto de la factura x Tasa de interés diaria x Días de atraso. El Administrador de Contratos emitirá un dictamen fundado dentro de los 10 (diez) días de recepción del pedido de cobro de mora, en la cual dictaminará si la falta de pago de la factura no sea imputable al contratista por falta de presentación de documentos u otros casos y si corresponde el monto aplicado en base a la fórmula mencionada. La Máxima Autoridad Institucional emitirá una resolución de autorización y la Gerencia Operativa de Contrataciones gestionará ante la DNCP el Código de Contratación específico para el pago de los intereses moratorios. Si el pago de la factura no se ha realizado, el Contratista podrá ejercer su derecho de suspensión del contrato (a partir de los 60 días) y presentará una solicitud de intereses devengados hasta esa fecha, sin perjuicio de la actualización posterior al momento del pago efectivo.

Caso Fortuito o 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 Caso fortuito o 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, embargos de cargamentos, explosiones, guerras, insurrección, movilización, huelgas, temblores de tierras y decisiones gubernamentales.
2. Para fines de esta cláusula, “Caso Fortuito” significa un evento extraordinario, imprevisto, inevitable, que imposibilita absolutamente el cumplimiento de la prestación y/u obligación. Cuando la previsión humana pueda anticipar el caso fortuito, el proveedor deberá acreditar haber empleado todos los recursos a su alcance para evitarlo y no se debe atribuir a la culpa o negligencia del mismo. Se debe tratar de un hecho externo al proveedor.
3. El proveedor deberá demostrar el nexo existente entre el caso notorio y la obligación pendiente de cumplimiento. El caso fortuito o la fuerza mayor solamente podrá afectar a la parte del contrato cuyo cumplimiento imposible fue demostrado.
4. Por consiguiente, no se considerarán como casos fortuitos o de Fuerza Mayor los actos o acontecimientos cuya ocurrencia podría preverse y cuyas consecuencias podrían evitarse actuando con diligencia razonable. De la misma manera, no se considerarán caso fortuito o fuerza mayor los actos o acontecimientos que hagan el cumplimiento de una obligación únicamente más difícil o más onerosa para la parte correspondiente.
5. Si se produjera un acontecimiento de Caso fortuito o fuerza mayor, el proveedor tendrá derecho a una prorroga razonable de los plazos de ejecución.
6. La parte que invoque fuerza mayor o caso fortuito deberá enviar una notificación sobre el caso a la otra parte, inmediatamente después que el acontecimiento sucedió y dentro del plazo máximo de siete (7) días calendarios a partir del día siguiente en que haya tenido conocimiento del evento o debiera haber tenido conocimiento del evento.
7. La notificación se enviará por nota o correo electrónico, estableciendo los elementos constitutivos del caso fortuito o la fuerza mayor y sus consecuencias probables para la ejecución del contrato, adjuntando toda la documentación comprobatoria. En todo caso, la parte afectada deberá tomar todas las medidas necesarias para conseguir, en el menor plazo posible, la reanudación normal de la ejecución de las obligaciones afectadas por el caso fortuito o fuerza mayor.
8. Cuando la parte que invoque el caso fortuito o la fuerza mayor sea el contratista, y esta no 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 o de fuerza mayor cuando el atraso de la comunicación se deba a causas no imputables al proveedor, debiendo el administrador del contrato emitir un dictamen fundado aceptando o rechazando la notificación fuera del plazo máximo establecido.
9. El caso fortuito o de fuerza mayor debe ser invocada con posterioridad a la suscripción del contrato y durante la vigencia del contrato, siempre y cuando el hecho haya ocurrido dentro del plazo de ejecución contractual.

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 caso fortuito o fuerza mayor existente.

Cuando una situación de fuerza mayor o caso fortuito ha existido durante un período de más de seis (6) meses, podrá ser causal de rescisión o terminación anticipada del contrato.

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.

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 regirán 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 regirán 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.

Si no fuere posible acordar los términos del convenio modificatorio, la contratante podrá ejercer sus derechos establecidos en el artículo 65 de la Ley N° 7021 de Suministro y de Contrataciones Públicas.

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

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. Si el proveedor no cumple con las obligaciones laborales, de seguridad social y/o de salud y seguridad ocupacional.
vii. 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 articulo 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:

La Contratante podrá terminar el Contrato además en los siguientes casos: además en los casos previstos en la Ley N° 7021/22. El incumplimiento de las leyes laborales, previsionales, tributarias o ambientales de los proveedores o contratistas, constatado mediante resolución administrativa de la autoridad competente, durante la ejecución de los contratos suscriptos y financiados con recursos provenientes del Presupuesto General de la Nación, será causal de rescisión del contrato por causa imputable al mismo.

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

Las controversias, diferencias o reclamos que se susciten entre las partes con motivo del presente contrato, su interpretación, ejecución, cumplimiento, resolución o terminación, y que sean susceptibles de transacción, conciliación o mediación, podrán ser sometidas de manera voluntaria a un procedimiento de mediación, conforme a lo dispuesto en la Ley N° 1879/2002 “De Mediación”, en la Ley N° 7021/2022 “De Suministro y Contrataciones Públicas”, y a las condiciones establecidas en el presente contrato.

El procedimiento de Mediación se podrá llevar a cabo ante:

- El Poder Judicial.

El mediador deberá pertenecer a las Listas del Poder Judicial o del CAMP, según la selección de sede establecida y actuará como tercero neutral e imparcial, de conformidad con la normativa aplicable.

El procedimiento de mediación se iniciará mediante solicitud de cualquiera de las partes y se sustanciará conforme al reglamento vigente de la sede seleccionada, el cual las partes declaran conocer y aceptar, incluyendo las disposiciones relativas a honorarios, gastos y costas, que se considerarán parte integrante de esta cláusula.

La mediación deberá concluir en un plazo máximo de treinta (30) días hábiles, contados a partir de la primera audiencia de mediación, plazo que podrá ser prorrogado por única vez, hasta por un período adicional de quince (15) días, únicamente mediante acuerdo expreso y escrito de las partes.

La mediación concluirá con la suscripción del acta de acuerdo, con la constancia de imposibilidad de acuerdo, o con la certificación correspondiente emitida por la sede de mediación. Vencido el plazo máximo sin haberse alcanzado un acuerdo, o concluido el procedimiento sin solución de consensuada, las partes quedarán habilitadas para recurrir a las instancias correspondientes. Para la homologación y ejecución del acta de mediación, así como para el conocimiento de las controversias no resueltas mediante este mecanismo, las partes se someten a la jurisdicción de los tribunales competentes de la ciudad de Asunción, República del Paraguay.

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:

- Tribunal colegiado

El o los árbitros designados deberán pertenecer a la lista del cuerpo arbitral del CAMP, que decidirá conforme a derecho, siendo el laudo definitivo y vinculante para las partes.

Todas las controversias que deriven del presente contrato o que guarden relación con éste serán resueltas definitivamente por arbitraje, conforme con las disposiciones de la Ley Nº 7021/22 "De Suministro y Contrataciones Públicas", de la Ley Nº 7.561 “De Arbitraje” y las condiciones del Contrato. Se aplicará el reglamento respectivo y demás disposiciones que regule dicho procedimiento al momento de ser requerido, declarando las partes conocer y aceptar los vigentes, incluso en orden a su régimen de gastos y costas, considerándolos parte integrante del presente contrato. Para la ejecución del laudo arbitral, o para dirimir cuestiones que no sean arbitrables, las partes se someterán a la jurisdicción de los tribunales de la ciudad de Asunción, República del Paraguay".

MODELO DE CONTRATO

Este modelo de contrato, constituye la proforma del contrato a ser utilizada de manera obligatoria, una vez adjudicado al proveedor y en los plazos dispuestos para el efecto por la normativa vigente, teniendo en cuenta que en los procedimientos de contratación cuyo objeto sea obras, locaciones o consultorías, deberán ser instrumentados mediante contratos y necesariamente deberán contar con una orden de inicio.

Así también, cuando en el procedimiento sea de menor cuantía y se deban emitir más de una orden de ejecución, independientemente al sistema de adjudicación, se deberá formalizar a través de un contrato, salvo aquellos casos previstos en el artículo 37 Inc. e) de la Ley N° 7021/22 ‘’De Suministro y Contrataciones Públicas’’

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.