

PLIEGO DE BASES Y CONDICIONES

Convocante:

**Banco Nacional de Fomento (BNF)
Uoc Bnf**

Nombre de la Licitación:

**ADQUISICION DE LICENCIAMIENTO DE SOFTWARE
DE SOPORTE TÉCNICO-ANTIVIRUS
(versión 1)**

ID de Licitación:

472694



Modalidad:

Subasta a la baja electrónica nacional

Publicado el:

17/10/2025

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

RESUMEN DEL LLAMADO

Datos de la Convocatoria

ID de Licitación:	472694	Nombre de la Licitación:	ADQUISICION DE LICENCIAMIENTO DE SOFTWARE DE SOPORTE TÉCNICO-ANTIVIRUS
Convocante:	Banco Nacional de Fomento (BNF)	Categoría:	43000000 - Tecnologías de Informacion, Telecomunicaciones y Radiodifusiones
Unidad de Contratación:	Uoc Bnf	Tipo de Procedimiento:	SBEN - Subasta a la baja electrónica nacional

Etapas y Plazos

Lugar para Realizar Consultas:	Sistema DNCP.	Fecha Límite de Consultas:	21/10/2025 12:00
Lugar de Entrega de Ofertas:		Fecha de Presentación de Ofertas Electrónicas e Inicio de la Etapa Competitiva:	27/10/2025 09:00
Lugar de Apertura de Ofertas:		Fecha de Apertura de Ofertas Electrónicas:	29/10/2025 09:15

Adjudicación y Contrato

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

Datos del Contacto

Nombre:	Silvio Eduardo Estigarribia Quiñones.	Cargo:	Gerente de la Gerencia Departamental Operativa de Contrataciones
Teléfono:	021 419 1466	Correo Electrónico:	contrataciones@bnf.gov.py

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 Sistema de Información de Contrataciones Públicas (SICP). Es responsabilidad del oferente examinar todos los documentos y la información de la convocatoria que obren en el mismo.

Contratación Pública Sostenibles - CPS

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

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

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

Criterios sociales y económicos:

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

Criterios ambientales:

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

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

Conducta empresarial responsable:

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

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

Aclaración de los documentos de la convocatoria

1. Consultas electrónicas

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

2. Respuestas y aclaraciones

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

3. Adendas y prórrogas del tope para consultas.

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

4. Emisión de aclaraciones sobre Adendas

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

5. Junta de aclaraciones

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

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

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

Reserva de Información en respuestas y 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".

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.

Formato y firma de la oferta

1. El formulario de oferta será presentado a través del Módulo de ofertas electrónicas, firmado electrónicamente 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. Cuando la Garantía de Mantenimiento de Oferta sea instrumentada mediante una Declaración Jurada, la misma estará exenta del requerimiento de certificación de firma por Escribano Público y será presentado a través del Módulo de Oferta Electrónica junto con el formulario de oferta.

Plazo para presentar las ofertas

Las ofertas electrónicas podrán ser cargadas y presentadas desde la publicación de la convocatoria hasta la fecha y hora límite de presentación de ofertas electrónicas e inicio de la etapa competitiva indicadas 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 presentación de ofertas electrónicas e inicio de la etapa competitiva.

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. La oferta podrá ser modificada o retirada hasta antes de la fecha y hora límite de presentación de ofertas electrónicas e inicio de la etapa competitiva

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:

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

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

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

2. En caso de que se establezca en las bases de la contratación, los precios indicados en el listado de precios serán consignados separadamente de la siguiente manera:

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

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

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

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

6. Una vez generada el Acta de Sesión Pública Virtual, el oferente, toda vez que haya realizado lances durante la etapa competitiva, deberá ajustar su listado de ítems al precio final de la competencia electrónica, a través del módulo de ofertas electrónicas, debiendo confirmar el precio ajustado de la oferta, hasta la fecha y hora prevista para el acto de apertura de ofertas electrónicas, para el efecto el SICP habilitará únicamente la modificación del precio unitario, los demás campos del ítem se mantendrán invariables.

7. 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 éste apartado se deberá indicar la manera de distribución de los mismos:

No Aplica

Moneda de la oferta y pago

La moneda de la oferta y pago será

En guaraníes para todos los oferentes

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

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 de perfil del proveedor.

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.

Periodo de validez de las ofertas

Las ofertas deberán mantenerse válidas por:

90

días corridos.

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

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

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

Garantías: instrumentación, plazos y ejecución

1. Instrumentación y porcentaje

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

- a. Garantía bancaria emitida por un banco establecido en la República del Paraguay, la que deberá ajustarse a las condiciones establecidas por la DNCP.
- b. Póliza de seguros emitida por una compañía autorizada a operar y emitir pólizas de seguros de caución en la República del Paraguay. La póliza deberá ajustarse a las condiciones establecidas por la DNCP.
- c. En las SBE inferiores a los dos mil (2.000) jornales mínimos, se admitirá la instrumentación de las garantías de mantenimiento de ofertas a través de Declaraciones juradas, que será presentada directamente a través del módulo de ofertas electrónicas, junto al formulario de oferta, suscripta electrónicamente. La garantía instrumentada mediante declaración jurada estará exenta del requerimiento de certificación de firmas.

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

1.3 En caso de instrumentarse las garantías a través de Garantía Bancaria, 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) La garantía de mantenimiento de ofertas será ejecutada y los antecedentes del caso serán remitidos a la DNCP, cuando un oferente susceptible de ser adjudicado, hubiere realizado lances y no hubiera confirmado el precio ajustado de la oferta, de acuerdo al acta de sesión pública virtual.
- b) Si el oferente altera las condiciones de su oferta,
- c) Si el oferente retira su oferta durante el período de validez de ofertas,
- d) Si no acepta la corrección aritmética del precio de su oferta, en caso de existir, o
- e) Si el adjudicatario no procede, por causa imputable al mismo a:
 - e.1 Firmar el contrato,
 - e.2 Suministrar los documentos indicados en las bases de la contratación para la firma del contrato,
 - e.3 Suministrar en tiempo y forma la garantía de cumplimiento de contrato,
 - e.4 Cuando se comprobare que las declaraciones juradas presentadas por el oferente adjudicado con su

oferta sean falsas,

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

4. En caso de configuración de Siniestro, la convocante deberá solicitar la ejecución de la garantía. El proceso de ejecución será según el tipo de garantía que haya sido suministrada.

Período de Validez de la Garantía de Mantenimiento de Oferta

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

120

días corridos

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

En el caso de que la competencia se desarrolle por más de un día, la garantía de mantenimiento de oferta deberá cubrir a partir del primer día del inicio de la etapa competitiva.

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

La carga y presentación de ofertas electrónicas se regirán por las disposiciones emitidas por la DNCP. Las ofertas electrónicas podrán ser cargadas y presentadas desde la publicación de la convocatoria hasta la fecha y hora límite de presentación de ofertas electrónicas e inicio de la etapa competitiva indicadas en el SICP.

En SBE no se admitirá el método de presentación de ofertas en doble sobre

Retiro, sustitución y modificación de las ofertas electrónicas

Un oferente podrá retirar, sustituir o modificar su oferta presentada, hasta antes de la fecha límite de presentación e inicio de etapa competitiva, para ello deberá sujetarse a la reglamentación pertinente.

Ajuste de Precios de Oferta Electrónica

El ajuste de precios se formaliza con la confirmación del precio ajustado de la oferta de acuerdo al acta de sesión pública virtual, constituyéndose el mismo una condición sustancial, caso contrario la oferta será rechazada.

Apertura de ofertas

Culminada la etapa de ajustes de precios de la oferta electrónica, se procederá a la apertura de las ofertas electrónicas, en el día y hora fijados en el SICP de conformidad a las disposiciones establecidas en la normativa vigente. La apertura de ofertas electrónicas podrá establecerse desde el día siguiente hábil al cierre de la etapa de competitiva y hasta tres (03) días hábiles posteriores al mismo.

Postergación de Presentación o Suspensión de la Etapa Competitiva

- 1. Postergación de la presentación de ofertas electrónicas:** Las convocantes podrán postergar la fecha de presentación de ofertas electrónicas e inicio de la etapa competitiva, hasta en dos (02) oportunidades, cuando llegada la fecha límite fijada para la presentación de ofertas e inicio de etapa competitiva no se hayan presentado oferta alguna.
- 2. Suspensión de la etapa competitiva:** La DNCP podrá disponer la suspensión de la etapa competitiva por motivos de fuerza mayor, con el fin de salvaguardar la prosecución del procedimiento. A dicho efecto, se procederá a la suspensión de la competencia y se publicará un aviso en el SICP con la información pertinente. La etapa competitiva será reanudada en el plazo que resulte conveniente para el desarrollo de la Subasta, con el grupo que no haya finalizado. Los demás plazos de la competencia serán prorrogados proporcionalmente, las nuevas fechas serán difundidas mediante un aviso en el SICP, de lo cual quedará constancia en el Acta de Sesión Pública Virtual

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:

- Presentar con la oferta autorización del fabricante expresamente dirigido a la entidad haciendo mención de la licitación específica y donde conste el nivel de partner o canal de la marca y que el oferente, se encuentra autorizado a proveer el servicio solicitado en la presente licitación.
- La Empresa oferente deberá ser como mínimo un Certificado Canal Oro o Platino de la Marca, para garantizar el buen servicio y respaldo del soporte local.
- El proveedor local deberá contar con el mayor nivel de certificación/partnership posible la marca ofertada, para garantizar el buen servicio y respaldo del soporte local.

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

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

Muestras

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

No Aplica

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

Tiempo de funcionamiento de los bienes

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

No Aplica

Plazo de reposición de bienes

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

No Aplica.

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:

No Aplica

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.

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 N° 7021/22. Esta declaración forma parte del formulario de oferta.

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

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

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

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

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

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

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

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

7° El comité verificará en fuentes públicas de información de libre acceso, si el oferente o sus integrantes, se encuentran en los demás supuestos contenidos en el artículo 21 de la Ley N° 7021/22, pudiendo utilizar como guía instructiva el documento aprobado por la DNCP. En caso de requerirse, el comité podrá solicitar aclaración al oferente sobre la vigencia de la información obrante en las fuentes respectivas.

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

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

Método de Evaluación

El método de evaluación del presente procedimiento de contratación será basado únicamente en precio.

Análisis de los precios ofertados

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

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

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

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

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

Composición de Precios

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

1	COSTO DE PRODUCTO
2	IMPUESTOS
3	GASTOS OPERACIONALES
4	GASTOS ADMINISTRATIVOS
5	UTILIDAD
6	PRECIO TOTAL

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

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

Certificado de Producto y Empleo Nacional - CPS

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

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

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

b) Oferentes en Consorcio:

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

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

consultorías, obras públicas y servicios relacionados a obras públicas).

Todos los integrantes del consorcio deben contar con el CPEN.

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

Requisitos documentales para evaluación de las condiciones de participación

Requisitos documentales para evaluación de las condiciones de participación

<p>1. Formulario de Oferta (*)</p> <p><i>[El formulario de oferta, deberá ser generado en el módulo de oferta electrónica y se considerará que el listado de ítems forma parte del formulario de oferta electrónica, y deberá sujetarse en todo lo demás a la reglamentación vigente.]</i></p>
<p>2. Garantía de Mantenimiento de Oferta (*)</p> <p><i>[La garantía de mantenimiento de oferta debe ser extendida, bajo la forma establecida en el SICP.</i></p>
<p>3. Certificado de Cumplimiento con la Seguridad Social (**)</p>
<p>4. Declaración jurada de conocimiento de la existencia de un conflicto de intereses respecto a los funcionarios públicos intervinientes en el procedimiento. (**)</p>
<p>5. Certificado de Producto y Empleo Nacional emitido por el MIC, en formato físico, solo en caso de imposibilidad de certificación electrónica. (**)</p>
<p>6. Certificado de Cumplimiento Tributario. (**)</p>
<p>7. Patente comercial del municipio en donde esté asentado el establecimiento del oferente. (**)</p>
<p>8. Declaración Jurada de “Declaración de Personas”, de conformidad con el formulario estándar – Sección Formularios, cuando no se encuentre en el Registro de Proveedores (**)</p>

9. Documentos legales. Oferentes
9.1. 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. (*)
9.2. 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. (*)
9.3. 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).
 - III. 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) (*).

9.4. 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).

En el Módulo de Oferta Electrónica, el oferente deberá cargar los datos en el Formulario de oferta electrónica de conformidad a la normativa vigente.

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

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

Los documentos indicados con doble asterisco (**) deberán estar vigentes a la fecha y hora tope de presentación de ofertas electrónicas e inicio de la etapa competitiva.

La falta de firma en documentos formales no será un motivo de descalificación, salvo que expresamente se disponga la exigencia de la firma del oferente en cuyo caso la omisión o desconformidad deberá analizarse conforme a los Artículos 77, 78 y 80 del Decreto 2264/24.

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

Capacidad Financiera

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

a. **Para contribuyente de IRACIS/IRE RG.**

Deberán cumplir el siguiente parámetro:

a. Ratio de Liquidez: activo corriente / pasivo corriente

Deberá ser igual o mayor que 1, en promedio, en los años (2022, 2023 y 2024)

b. Endeudamiento: pasivo total / activo total

No deberá ser mayor a 0,80 en promedio, en los años (2022, 2023 y 2024)

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

El promedio de los años (2022, 2023 y 2024) no deberá ser negativo

b. **Para contribuyente de IRPC/IRE SIMPLE o IRACIS/IRE SIMPLE**

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso)

Deberá ser igual o mayor que 1, en promedio, en los años (2022, 2023 y 2024)

c. **Para contribuyente de IRP/IRP RSP**

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso)

Deberá ser igual o mayor que 1, en promedio, en los años (2022, 2023 y 2024)

d. **Para contribuyentes de exclusivamente IVA General**

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso)

Deberá ser igual o mayor que 1, en promedio, en los años (2022, 2023 y 2024)

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

Observación: Si en alguno de los tres años, o los tres años presentados por la Empresa, su pasivo es igual a 0, se considerará el Ratio de Liquidez igual a 1 y se dará por cumplido el Ratio de Endeudamiento. Esta salvedad en el PBC hace posible calcular el promedio del índice de liquidez de los 3 (tres) ejercicios analizados, debido a que se otorga un valor que puede ser promediado.

Requisitos documentales para la evaluación de la capacidad financiera

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

a. Balance General y Cuadro de Estado de Resultados de los tres años (2022, 2023 y 2024) para contribuyente de **IRACIS/IRE RG.**

b. IVA General de 36 (treinta y seis) meses (2022, 2023 y 2024), para contribuyentes sólo del IVA General.

c. Formulario 106 IRPC, Formulario 501 IRE Simple de los 3 (tres) años (2022, 2023 y 2024) para contribuyentes del **IRPC/IRE SIMPLE o IRACIS/IRE SIMPLE.**

d. **Formulario 104 IRP, Formulario 515 IRP-RSP** de los 3 (tres) años (2022, 2023 y 2024) para contribuyentes de **IRP/IRP-RSP**

Experiencia requerida

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

1. Demostrar la experiencia en **actualización de Software Kaspersky** con facturaciones de venta, contratos y/o recepciones finales, por un monto equivalente al 25% como mínimo del monto total ofertado en el presente procedimiento de contratación, de los últimos 3 (tres) años (2022, 2023, 2024). Las sumatorias de las facturaciones deben alcanzar el porcentaje indicado, no será necesaria la presentación del porcentaje del monto establecido por cada año.
2. Demostrar la experiencia en **plataforma de Detección y Respuesta Extendida (XDR)** con facturaciones de venta, contratos y/o recepciones finales, por un monto equivalente al 25% como mínimo del monto total ofertado en el presente procedimiento de contratación, de los últimos 3 (tres) años (2022, 2023, 2024). Las sumatorias de las facturaciones deben alcanzar el porcentaje indicado, no será necesaria la presentación del porcentaje del monto establecido por cada año.
3. 3 (tres) Constancias emitidas por empresas Públicas y/o Privadas en las cuales manifieste que el oferente ha provisto y/o actualización de Software Kaspersky, en los últimos 3 (tres) años (2022, 2023, 2024)

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 contratos, facturaciones y/o recepciones finales que avalen la experiencia requerida.
2. Copia de contratos, facturaciones y/o recepciones finales que avalen la experiencia requerida.
3. 3 (tres) Constancias emitidas por empresas Públicas y/o Privadas ha proveído y/o actualización de Software Kaspersky, en los últimos 3 (tres) años (2022, 2023, 2024)

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 contar con **personal técnico propio** con formación y experiencia comprobable en soluciones de **seguridad endpoint corporativa** (Kaspersky o equivalente), debiendo acreditar las siguientes condiciones mínimas:

- Contar por lo menos con 1 técnico con certificación en Detección y Respuesta de Endpoints (EDR) a fin de garantizar el correcto despliegue y configuración de los módulos EDR
- Contar por lo menos con 1 técnico certificado con las certificaciones avanzadas del producto de detección y respuesta extendida XDR.
- Contar por lo menos con 1 técnico con certificaciones en soluciones de protección para entornos híbridos o virtualizados a fin de garantizar la correcta implementación de los appliances virtuales para proteger los entornos virtualizados de los desktops.
- Contar como mínimo con 1 ingeniero con certificaciones ITIL para garantizar la buena asistencia en soporte técnico.

1. El oferente debe contar con la Certificación ISO 9001: Sistema de Gestión de Calidad
2. El oferente debe contar con la Certificación ISO 27001: Sistema de Gestión de Seguridad de la Información.

OBS.: Un mismo técnico puede contar con una, varias o el total de certificaciones

Requisitos documentales para evaluar el criterio de capacidad técnica

1. Los técnicos certificados deben ser personales dependientes del oferente, se deben presentar planilla de IPS y/o certificados de inscripción en IPS, acompañados de copia simples de las certificaciones requerida en el punto 1.
2. El oferente debe presentar copia simple de la Certificación ISO 9001: Sistema de Gestión de Calidad
3. El oferente debe presentar copia simple de la Certificación ISO 27001: Sistema de Gestión de Seguridad de la Información.

Otros criterios que la convocante requiera

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

Para Personas Jurídicas u Oferentes en Consorcio.

* Copias simples de las Constancias del Registro de Personas y Estructuras Jurídicas, y las Constancias del Registro de Beneficiarios Finales, dispuestas por la Ley N° 6446/2019, Decreto Reglamentario N° 3241 del 10/01/2020 y la Resolución N° 202/2020 del 17/09/2020 de la Secretaría de Prevención de Lavado de Dinero o Bienes SEPRELAD.

Para los oferentes consorciados:

a. CAPACIDAD FINANCIERA	Los índices financieros deberán ser cumplidos el 100% por cada uno de los integrantes.
b. EXPERIENCIA Y CAPACIDAD TÉCNICA	Todas las partes combinadas deberán cumplir con el 100% de los requisitos solicitados.

c. CALIFICACIÓN LEGAL	El socio líder y cada socio deberá cumplir con el 100% de lo exigido
--------------------------	---

OTROS DOCUMENTOS A PRESENTAR PARA LA FIRMA DEL CONTRATO:

De conformidad al Art. 33 de la Resolución N° 70 de la SEPRELAD, el oferente adjudicado deberá proveer los datos y documentos respaldatorios solicitado en la misma.

Aclaración de las ofertas

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

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

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

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

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

Disconformidad, 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.

Para los casos de ajustes de precios de las ofertas electrónicas, toda vez que se hayan realizado lances durante la etapa competitiva, el oferente deberá ajustar su listado de ítems al precio final de la competencia electrónica, a través del módulo de ofertas electrónicas.

Si como consecuencia del resultado de la división del precio total subastado respecto a la cantidad, se obtuviere una cifra con decimales, se deberá realizar el redondeo del mismo hacia abajo, de modo a que el precio total no supere al que figure en el Acta de Sesión Pública Virtual como precio final, conforme al sistema de adjudicación establecido (ítem, lote, total).

En la consignación de los precios unitarios finales, el oferente no podrá aumentar el precio unitario cargado inicialmente para la presentación de ofertas electrónicas e inicio de la etapa competitiva.

En caso de que el oferente no haya realizado lance durante la etapa competitiva, los precios permanecerán invariables.

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 vencedor de cada grupo subastado será el que lo haya ingresado primero.

Siempre que el criterio de desempate establecido, no sea aplicable, 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.

Notificación del resultado

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

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

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

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

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

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

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

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.

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.

Audiencia Informativa

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

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

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

SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS

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

Suministros y Especificaciones técnicas.

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

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

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

Nombre, cargo y la dependencia de la Institución de quien solicita el llamado a ser publicado: Hugo Manuel Centurion Florencio, Gerente - Gerencia Departamental de Seguridad Lógica.

Justificación de la necesidad que se pretende satisfacer mediante la contratación a ser realizada: El Banco Nacional de Fomento, tiene la imperiosa necesidad disponer de un software de antivirus, a fin de disponer de una herramienta que cubra la posibilidad de ser afectado por cualquier tipo de virus. Es importante mencionar, la importancia del mismo, pues minimiza en gran manera, el riesgo de ser atacado por virus, que traerá consecuencias desastrosas para nuestra institución.

Justificar la planificación: se trata de un llamado periódico

Justificar las especificaciones técnicas establecidas: Las EETT establecidas, para el presente llamado, son las especificaciones que consideramos necesarias, pues se ajustan a las necesidades de nuestro banco, en materia de antivirus.

Especificaciones Técnicas "CPS"

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

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

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

Ítem N°	Descripción	Cantidad	Unidad de Medida	Presentación
1	ADQUISICIÓN DE LICENCIAMIENTO DE SOFTWARE DE SOPORTE TÉCNICO ANTIVIRUS, conforme a las EETT.	1	Unidad	Unidad

ESPECIFICACIONES TÉCNICAS

El objeto de estas especificaciones es la actualización, ampliación y soporte de las licencias de Software de Ciberseguridad (Antivirus) Kaspersky que la Entidad tiene actualmente instaladas y registradas a favor del Banco Nacional de Fomento. Las licencias comprenden una suite de soluciones de seguridad principalmente para Estaciones de Trabajo, Buzones de Correo Corporativo, dispositivos móviles y aplicaciones. Las nuevas licencias a ser provistas deberán tener una vigencia de doce (12) meses y deberán cubrir un total de dos mil quinientos (2.500) dispositivos.

ESPECIFICACIONES TÉCNICAS	MÍNIMO EXIGIDO	CUMPLE CON LAS ESPECIFICACIONES REQUERIDAS (SI/NO)
PLATAFORMA DE DETECCIÓN Y RESPUESTA EXTENDIDA XDR		
Se debe proveer una solución tecnológica para la detección, prevención, contención y respuesta ante ataques sofisticados y evasivos, con connotación de dirigidos y avanzados basados en software malicioso (Malware) moderno, integrada con software de objetivo específico que detecte objetos sospechosos de red, correo electrónico, web y endpoints.	EXIGIDO	
La solución debe proporcionar visibilidad sobre los diferentes componentes de la infraestructura y disponer de capacidad de correlación de eventos y automatización. También debe contar con una amplia gama de herramientas de respuesta y obtención de telemetría a través de múltiples fuentes de datos.	EXIGIDO	
La solución debe analizar los datos de múltiples fuentes para identificar amenazas, crear alertas para posibles incidentes y proporcionar las herramientas para responder a ellos.	EXIGIDO	
La solución debe proporcionar un proceso unificado de detección y respuesta a través de componentes integrados y escenarios holísticos para mejorar la eficiencia de los profesionales de la seguridad.	EXIGIDO	
La solución debe incluir, al menos, las siguientes capacidades de detección:	EXIGIDO	

Herramientas de búsqueda de amenazas para buscar de forma proactiva amenazas y vulnerabilidades mediante el análisis de eventos.	EXIGIDO	
Detección avanzada de amenazas y correlación cruzada: correlación en tiempo real de eventos de diferentes fuentes.	EXIGIDO	
Un gráfico de investigación para visualizar y facilitar la investigación de un incidente e identificar las causas fundamentales de la alerta.	EXIGIDO	
Uso de Inteligencia de Amenazas para obtener la información detallada más reciente sobre amenazas, por ejemplo, sobre direcciones web, dominios, direcciones IP, hashes de archivos, datos estadísticos y de comportamiento, y datos de WHOIS y DNS.	EXIGIDO	
Respecto a la recolección de datos, la solución debe disponer un normalizador (parser) nativo para sus colectores que soporte el formato JSON. El normalizador ya debe existir dentro de la solución, no se aceptará que sea construido en forma customizada.	EXIGIDO	
Como acciones de respuesta la solución debe incluir mínimamente:	EXIGIDO	
Acciones de respuesta manuales: aislamiento de endpoints, ejecución de comandos, creación de reglas de prevención y lanzamiento de tareas en un endpoint.	EXIGIDO	
Playbooks, tanto predefinidos como creados por el usuario, para automatizar operaciones de respuesta típicas.	EXIGIDO	
Acciones de respuesta de productos de terceros y escenarios de respuesta entre productos.	EXIGIDO	
La solución debe contar con, al menos, las siguientes capacidades referente a la gestión de activos y la ejecución centralizada de tareas de administración y mantenimiento de seguridad:	EXIGIDO	
Ejecución remota de tareas de escaneo y actualización.	EXIGIDO	
Obtención de información detallada sobre la protección de activos.	EXIGIDO	
Configuración de todos los componentes de seguridad a nivel endpoint.	EXIGIDO	

La solución de XDR debe contar con capacidades de Gestión de Activos Centralizada. Además, debe brindar información completa referente a los activos como: hardware, sistema operativo, software instalado, vulnerabilidades, direcciones IP, entre otros.	EXIGIDO	
La solución debe permitir la agrupación de diferentes alertas de múltiples fuentes en un único incidente, para facilitar su gestión e investigación.	EXIGIDO	
La solución debe contar con la capacidad de integración de forma nativa con proveedores de tecnología, ciberseguridad y terceras partes que permitan un amplio ecosistema de integraciones de diversas tecnologías.	EXIGIDO	
La solución debe disponer de, al menos, 150 integraciones de forma nativa mediante conectores out-of-the-box (predefinidos).	EXIGIDO	
La solución debe permitir la integración con los siguientes protocolos y tecnologías mínimamente: TCP, UDP, Netflow, sflow, nats-jetstream, Kafka, HTTP, SQL, FTP, NFS, WMI, WEC, SNMP y SNMP-TRAP.	EXIGIDO	
La solución debe permitir la integración con los siguientes tipos de datos mínimamente: XML, Syslog, CSV, JSON, SQL, IPFIX, CEF, Netflow 5 y Netflow 9.	EXIGIDO	
La solución debe proporcionar una API abierta, que permita la implementación de escenarios de integración personalizados en la plataforma.	EXIGIDO	
La solución de XDR debe disponer de una consola de gestión 100% Web on-premise que permita la administración de manera integral, facilitando la gestión de la seguridad y detección de amenazas modernas y ataques dirigidos. No se contemplarán soluciones cuya plataforma de gestión sea nube.	EXIGIDO	
La solución debe disponer de capacidad de análisis en un entorno virtual on-premise (SandBox), con el objetivo de detectar ataques dirigidos, crear información sobre amenazas en tiempo real y capturar información detallada de las interacciones y comportamiento de las amenazas modernas detectadas y su análisis de causa raíz, así como también evidencias forenses.	EXIGIDO	
Deberá detectar todas las fases de los ataques modernos: exploit, infección a partir de código malicioso, y comunicación a servidores de comando y control (Callback); para permitir un análisis del ciclo de vida completo del ataque.	EXIGIDO	

La solución debe poder ejecutarse en hardware de diferentes fabricantes, así como en entornos virtualizados con soporte a hipervisor VMWare, y deberá presentar el riesgo asociado a cada una de las amenazas, indicando el nivel de importancia.	EXIGIDO	
Deberá detectar y proteger ataques del tipo malware, botnets y amenazas dirigidas que permita identificar amenazas modernas, así como también brindar acceso a información de inteligencia de amenazas en tiempo real.	EXIGIDO	
Debe utilizar una red de inteligencia de amenazas y debe disponer de acceso a una base de reputación.	EXIGIDO	
Debe actuar en tiempo real, ejecutando un análisis profundo y completo de las amenazas y generando información catalogada a nivel de usuario, IP, nombre de la amenaza, severidad, cantidad de infecciones y cantidad de callbacks así como también información detallada del comportamiento de la amenaza:	EXIGIDO	
Capacidades nocivas de la amenaza: comportamiento malicioso, cambios realizados al sistema operativo, identificación de comandos raw asociados al software malicioso.	EXIGIDO	
Información mínima de cada equipo afectado: cantidad, tipo, nombre, severidad, dirección IP del servidor de Comando y control, fecha y hora de detección, geolocalización, puertos usados.	EXIGIDO	
Punto de acceso que genere la infección.	EXIGIDO	
En caso de malware desconocido, debe proporcionar la siguiente información: SHA-256/MD5, tipo de archivo, protocolo usado, cantidad de ocurrencias, ejecutable del malware.	EXIGIDO	
La solución debe contar con una API para la integración con otras plataformas y herramientas, al igual que debe detectar en tiempo real malware desconocido usando reglas personalizadas por terceras partes vía Yara.	EXIGIDO	
Los eventos generados deben ser retenidos por un periodo de tiempo establecido y por tipo a ser almacenado en una base de datos por un periodo superior a los 100 días.	EXIGIDO	
Debe identificar variaciones en el patrón de comportamiento de usuarios y procesos en los endpoints así como la identificación de variación en el patrón de comportamiento relacionado al acceso a dominios sospechosos, y el resultado del análisis debe indicar que modulo detectó la amenaza: motor de AV, reputación de archivos, sandbox, etc.	EXIGIDO	

Debe contar con un motor de antivirus basado en firmas, heurística y soporte de una red privada de inteligencia pudiendo analizar archivos protegidos por contraseña basado en diccionario a poder ser establecido por los administradores de la solución y que conste por lo menos de hasta 30 palabras.	EXIGIDO	
Debe soportar la ejecución e inspección de los siguientes tipos de archivos: documentos de la suite MS Office (en todas sus versiones), documentos PDF, archivos ejecutables, archivos compuestos (Ejemplo. Zip,Rar) y archivos multimedia en el entorno de Sandbox al igual que tener la capacidad de detectar amenazas avanzadas que se aprovecha de vulnerabilidades conocidas y/o sitios web maliciosos sin necesidad de acudir a la nube del proveedor.	EXIGIDO	
Debe disponer de un conjunto de reglas de detecciones, predefinidas y/o personalizables, que permitan asociar y correlacionar diferentes eventos o información de telemetría para identificar un ataque.	EXIGIDO	
La plataforma de detección y respuesta extendida XDR debe contar con técnicas de detección de evasión de máquinas virtuales y con tecnología propietaria de Sandbox	EXIGIDO	
El proceso de detección de malware del entorno virtual deberá ser capaz de efectuar:	EXIGIDO	
Análisis dinámico de comportamiento.	EXIGIDO	
Análisis de patrones y firmas.	EXIGIDO	
Detección de malware de tipo día cero.	EXIGIDO	
Debe poder identificar comunicaciones que pudieran ser relacionadas con llamadas de comando y control.	EXIGIDO	
Debe registrar toda la actividad que un objeto malicioso trate de ejecutar, acción ejecutada en ambientes de máquinas virtuales, presentando las modificaciones sobre el sistema operativo o aplicación que logre modificar:	EXIGIDO	
Registro de Windows	EXIGIDO	
Registro de la aplicación	EXIGIDO	
Registro de procesos	EXIGIDO	

Registro de archivos	EXIGIDO	
Registro de comportamiento	EXIGIDO	
Registro de comunicaciones	EXIGIDO	
Dispondrá de la capacidad para evaluar y analizar, mediante máquinas virtuales o técnicas de emulación, amenazas sobre los sistemas operativos preconfigurados con: MS Windows 7 x86, MS Windows 7 x64, Windows 10 y Linux.	EXIGIDO	
En el entorno virtual de análisis, el malware deberá ser inspeccionado y examinado en máquinas virtuales correspondientes a varios sistemas operativos, aplicaciones, navegadores y complemento de navegadores.	EXIGIDO	
La solución debe ser capaz de ejecutar todo el código sospechoso, URL's y diversos tipos de archivos en un entorno virtual propietario de inspección.	EXIGIDO	
Contará con una solución de sandbox que no debe de ser de tecnología OEM o Software Libre, debe de soportar malware de 32-Bit y 64-Bit en modo usuario y kernel, y debe analizar como mínimo .exe, .dll, archivos de MS office, .pdf y archivos flash, disponiendo de capacidad de identificación de extensiones de archivos que han sido modificados	EXIGIDO	
La plataforma de Sandbox debe incluir todas las licencias necesarias tanto a nivel de sistema operativo como software instalado, incluido todas las licencias necesarias de MS Office y de otros proveedores.	EXIGIDO	
La plataforma de Sandbox facilitara la descarga de dumps de memoria para la realización de análisis forenses y ser capaz de monitorizar y decodificar en caso de estar cifrado el tráfico generado por la muestra analizada.	EXIGIDO	
La plataforma de Sandbox proporcionará información en detalle de la actividad de una muestra dentro de la máquina virtual.	EXIGIDO	
La plataforma de Sandbox podrá proporcionar canales de comunicación alternativos para que las muestras puedan interactuar en tiempo real con dominios externos, descargar módulos, de manera directa.	EXIGIDO	
Debe contar con análisis de AV, de reputación de archivos, reputación de URLs y categoría de aplicaciones, así como incluir integración con Portal de Inteligencia de Amenazas.	EXIGIDO	

La solución debe ser capaz de ejecutar el código sospechoso, acceso URL's y diversos tipos de archivos en un entorno virtual de inspección dentro del mismo dispositivo. Para ello realizará tanto análisis estático (basado en reglas) como dinámico (basado en comportamiento).	EXIGIDO	
Debe detectar la amenaza sin necesidad de conocer la firma, es decir, a través del comportamiento de la propia amenaza y proporcionar detección en las comunicaciones desde y hacia los servicios de internet, contra los ataques de malware de día cero, exploits, botnets y ataques dirigidos.	EXIGIDO	
Debe registrar y almacenar evidencia de la ejecución de malware moderno y ataques dirigidos en el entorno virtual de inspección, tales como: direcciones IP, protocolos empleados, etc., y brindar la siguiente información como mínimo, por cada una de las amenazas detectadas por malware en entorno de Sandbox:	EXIGIDO	
Fecha y hora del ataque	EXIGIDO	
Hash MD5/SHA-256. de los binarios maliciosos	EXIGIDO	
Tipo de archivo malicioso detectado	EXIGIDO	
URL/IP de infección	EXIGIDO	
Capacidades nocivas de la amenaza: capacidades de robo de información, comportamiento malicioso, cambios al sistema operativo	EXIGIDO	
Guardar una copia del malware	EXIGIDO	
Debe ser capaz de analizar archivos adjuntos incluidos en los correos electrónicos inclusive aquellos que estén comprimidos, así como direcciones URL que se encuentren en el cuerpo del correo.	EXIGIDO	
El entorno de Sandbox debe poder procesar al menos 10,000 objetos al día y poder escalar lateral y verticalmente, y en el caso de escalabilidad lateral, todos los nodos reportaran a una misma consola central.	EXIGIDO	
El oferente deberá proveer todo necesario y asociado para la implementación on-premise y el correcto funcionamiento de la solución XDR.	EXIGIDO	
Componente EDR con capacidades EPP		

Se debe proveer una solución de EDR avanzado que permita la detección de ataques conocidos y desconocidos, amenazas avanzadas y sofisticadas. A su vez, esta misma solución debe incorporar de forma nativa un EPP para reducir la superficie de ataque a nivel de host, mediante la aplicación de controles como Control de Aplicación, de Navegación, Firewall, Gestión de Parches y Vulnerabilidades y Cifrado nativo.	EXIGIDO	
Tanto la solución de EDR y EPP como de XDR, deben ser del mismo fabricante para facilitar la integración y comunicación entre los diferentes segmentos de la infraestructura corporativa. No se contemplarán soluciones que no brinden capacidades de EPP, EDR y XDR o sean de diferentes fabricantes.	EXIGIDO	
Debe contar con una consola de administración on-premise accesible vía Web (HTTPS.) y MMC basado en roles y perfiles de acceso, con capacidades granulares de definición de restricciones y capacidades funcionales, y adicionalmente debe contar con segundo factor de autenticación (2FA) para el acceso a la consola de administración compatible con Microsoft Authenticator y Google Authenticator. No se contemplarán soluciones cuya plataforma de gestión sea nube.	EXIGIDO	
La solución debe de poseer servicio de clustering nativo.	EXIGIDO	
Debe poder eliminar remotamente cualquier solución de seguridad (propia o de terceros) que esté presente en las estaciones y servidores, sin la necesidad de la contraseña de la actual solución de seguridad. Adicionalmente la solución debe de poder desinstalar remotamente cualquier software instalado en las máquinas clientes.	EXIGIDO	
Debe poder instalar remotamente la solución en las estaciones y servidores Windows y Linux con capacidades nativas de la solución sin depender de soluciones de terceras partes, a través de la administración compartida, login script y/o GPO de Active Directory.	EXIGIDO	
Debe gestionar estaciones de trabajo y servidores tanto Windows, Linux y macOS, así como dispositivos móviles Android y iOS.	EXIGIDO	
Debe poder realizar la distribución remota de cualquier software, o sea, debe ser capaz de remotamente enviar cualquier software por la estructura de gerenciamiento de antivirus para que sea instalado en las máquinas clientes; y de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones base de la solución.	EXIGIDO	
Debe aplicar actualizaciones y parches de Windows y de terceras partes remotamente en las estaciones de trabajo y servidores.	EXIGIDO	

Dispondrá de capacidad de borrado remoto de datos (Remote Wipe), con posibilidad de establecer criterios selectivos y condiciones para la ejecución de regla de eliminación de datos en equipamiento bajo OS Windows	EXIGIDO	
Tendrá la capacidad de vuelta atrás automática para poder revertir en tiempo real las acciones maliciosas producidas por una amenaza como, por ejemplo, un ransomware.	EXIGIDO	
La solución de seguridad para servidores y escritorios debe de proporcionar soporte a OS Windows como Linux.	EXIGIDO	
Debe, al detectar máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antivirus instalado. En caso de no tenerlo, debe instalar el antivirus automáticamente. Adicionalmente debe de poder importar la estructura de equipos desde el Active Directory.	EXIGIDO	
Debe poder realizar el agrupamiento de máquinas por características comunes entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antivirus instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 2 días, etc.	EXIGIDO	
Debe definir políticas de configuraciones diferentes por grupos de estaciones, permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos.	EXIGIDO	
Debe proporcionar las siguientes informaciones de las computadoras:	EXIGIDO	
Si el antivirus está instalado	EXIGIDO	
Si el antivirus ha iniciado	EXIGIDO	
Si el antivirus está actualizado	EXIGIDO	
Minutos/horas desde la última conexión de la máquina con el servidor administrativo.	EXIGIDO	
Minutos/horas desde la última actualización de firmas.	EXIGIDO	
Fecha y horario de la última verificación ejecutada en la máquina.	EXIGIDO	
Versión del antivirus instalado en la máquina.	EXIGIDO	

Si es necesario reiniciar la computadora para aplicar cambios.	EXIGIDO	
Fecha y horario de cuando la máquina fue encendida.	EXIGIDO	
Cantidad de virus encontrados (contador) en la máquina.	EXIGIDO	
Nombre de la computadora.	EXIGIDO	
Dominio o grupo de trabajo de la computadora.	EXIGIDO	
Fecha y horario de la última actualización de firmas.	EXIGIDO	
Sistema operativo con Service Pack.	EXIGIDO	
Cantidad de procesadores.	EXIGIDO	
Cantidad de memoria RAM.	EXIGIDO	
Usuario(s) conectados en ese momento, con información de contacto (si están disponibles en el Active Directory).	EXIGIDO	
Dirección IP.	EXIGIDO	
Aplicativos instalados, inclusive aplicativos de terceros, con historial de instalación, conteniendo fecha y hora que el software fue instalado o removido.	EXIGIDO	
Actualizaciones de Windows Updates instaladas.	EXIGIDO	
Información completa de hardware conteniendo: procesadores, memoria, adaptadores de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD.	EXIGIDO	
Vulnerabilidades de aplicativos instalados en la máquina.	EXIGIDO	
Debe permitir bloquear las configuraciones del antivirus instalado en las estaciones y servidores de manera que el usuario no consiga modificarlas.	EXIGIDO	

Debe reconectar máquinas clientes al servidor administrativo más próximo, basado en reglas de conexión como:	EXIGIDO	
Cambio de Gateway.	EXIGIDO	
Cambio de subnet DNS.	EXIGIDO	
Cambio de dominio.	EXIGIDO	
Cambio de servidor DHCP.	EXIGIDO	
Cambio de servidor DNS.	EXIGIDO	
Cambio de servidor WINS.	EXIGIDO	
Aparición de nueva subnet.	EXIGIDO	
Debe configurar políticas móviles para que cuando una computadora cliente esté fuera de la estructura de protección pueda actualizarse y gestionarse vía internet.	EXIGIDO	
Debe poder realizar la herencia de tareas y políticas en la estructura jerárquica de servidores administrativos.	EXIGIDO	
Debe elegir cualquier computadora cliente como repositorio de actualizaciones y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red.	EXIGIDO	
Debe exportar informes para los siguientes tipos de archivos: PDF, HTML y XML.	EXIGIDO	
Debe enviar correos electrónicos para cuentas específicas en caso de algún evento, así como traps SNMP para el monitoreo de eventos.	EXIGIDO	
Debe habilitar automáticamente una política en caso de que ocurra una epidemia en la red (basado en cantidad de virus encontrados en determinado intervalo de tiempo).	EXIGIDO	
Debe realizar actualización incremental de firmas en las computadoras clientes.	EXIGIDO	

Debe realizar inventario de hardware y software de todas las máquinas clientes.	EXIGIDO	
La solución deberá ser capaz de detectar amenazas de día cero (zero-day malware) y Amenazas Persistentes Avanzadas (APT).	EXIGIDO	
La solución permitirá la monitorización y captura de eventos de red relacionados a las actividades en PCs y servidores.	EXIGIDO	
El agente EDR de Windows & Linux debe ser capaz de coleccionar datos puntuales para un equipo determinado con el fin de obtener las evidencias para un posterior análisis forense.	EXIGIDO	
La instalación del sensor EDR en los equipos Windows debe ser de forma transparente para el usuario final con el objetivo de minimizar el impacto en la gestión del cambio de la organización.	EXIGIDO	
La solución debe poder tomar entradas para indicadores personalizados de compromiso en formato IOC.	EXIGIDO	
Los datos forenses deben ser en tiempo real y exhaustivo, mostrando el nivel de compromiso y permitiendo a los administradores tomar decisiones de negocio.	EXIGIDO	
La solución debe proporcionar varios paneles personalizables para proporcionar información sobre la actividad de los sistemas y resultados analíticos, que incluyen: actividad y estado del sistema, longitudes de cola, eventos registrados, su estado y las tecnologías utilizadas para proporcionar veredictos, listas de IP, dominios y correos electrónicos más frecuentemente relacionado con incidentes.	EXIGIDO	
La solución debe disponer de capacidad de integración con solución de sandbox proporcionada por la Plataforma de Detección y Respuesta Extendida XDR local el cual permita examinar objetos utilizando múltiples instancias de sandbox en modo cluster para mejorar el tiempo de respuesta y la escalabilidad.	EXIGIDO	
La solución debe ser capaz de proporcionar datos forenses detallados del objeto malicioso adjunto. Los datos forenses deben incluir, entre otros:	EXIGIDO	
Binarios de malware asociado	EXIGIDO	
Cualquier cambio en el sistema operativo host.	EXIGIDO	
Cualquier cambio a la memoria.	EXIGIDO	

Cualquier cambio en el sistema de archivos.	EXIGIDO	
Cualquier cambio a la puesta en marcha del sistema.	EXIGIDO	
La solución debe permitir incluir IOCs en lista negra privada de inteligencia bajo formato MD5 / SHA256.	EXIGIDO	
La solución debe proporcionar una visibilidad completa con sus capacidades forenses, monitoreo y registro de eventos de puntos finales, archivos afectados, procesos iniciados, cambios en el registro del sistema y actividad de la red.	EXIGIDO	
La solución debe tener la capacidad de detección y respuesta para eliminar el enfoque tradicional del equipo de seguridad (detecta, notifica y resuelve manualmente).	EXIGIDO	
La solución debe ser capaz de integrarse con plataformas de SIEM para la administración de logs.	EXIGIDO	
La solución debe tener diferentes funciones de administrador que tengan una única interfaz / panel durante el inicio de sesión y controladas por privilegios y funciones (Administrador, Revisor, Investigador, etc.).	EXIGIDO	
La extracción de muestras debe escanearse utilizando el laboratorio de virus interno, sin enviar la muestra fuera de la red almacenando los datos forenses dentro de la plataforma con un mínimo de 100 días.	EXIGIDO	
El componente de Sandbox deberá tener la capacidad de escanear y ejecutar los archivos recopilados desde cualquier endpoint - por el agente EDR, en un ambiente aislado para un análisis profundo.	EXIGIDO	
El módulo de sandbox debe poder analizar cualquier tipo de archivo mediante el uso de múltiples aplicaciones y múltiples versiones, que incluyen, entre otros: exe, dll, pdf, doc, docx, xls, xlsx, gif, jpeg, png, tiff, swf, mov, qt, mp4, jpg, mp3, asf, ico, htm, url, rm, com, vcf, ppt, rtf, chm, hlp y otros debiendo ser capaz de lidiar con las técnicas de evasión de VM.	EXIGIDO	
La solución debe tener la capacidad de verificar / ejecutar un análisis en todos los hosts para cualquier nombre de archivo, extensión de archivo, archivo MD5 / SHA1 o IOC provisto.	EXIGIDO	
La solución debe ser capaz de detectar el ataque localmente, sin depender de un servicio en la nube.	EXIGIDO	

Las capacidades de respuesta deben de incluir aislamiento de los equipos afectados acorde a reglas personalizables.	EXIGIDO	
La solución debe contar con gateway de conexión para gestión centralizada on-premise de equipos que se encuentren fuera de la red corporativa.	EXIGIDO	
La solución debe contar con una arquitectura basada en puntos de distribución / actualización para el despliegue de: Actualizaciones, parches y Paquetes de Software en entornos WAN para reducir la utilización de ancho de banda.	EXIGIDO	
La solución debe de disponer compatibilidad mínimamente con los siguientes sistemas operativos:	EXIGIDO	
Windows 7 SP1 y superior	EXIGIDO	
Windows 8	EXIGIDO	
Windows 8.1	EXIGIDO	
Windows 10	EXIGIDO	
Windows 11	EXIGIDO	
MacOS 11.14 o superior.	EXIGIDO	
Microsoft Windows Server 2008 SP1.	EXIGIDO	
Microsoft Windows Server 2012 y 2012 R2.	EXIGIDO	
Microsoft Windows Server 2016.	EXIGIDO	
Microsoft Windows Server 2019.	EXIGIDO	
Microsoft Windows Server 2022.	EXIGIDO	
CentOS 6.7 y superior.	EXIGIDO	
Debian GNU / Linux 10.1 y superior.	EXIGIDO	

Linux Mint 19.2 y superior.	EXIGIDO	
Red Hat Enterprise Linux 6.7 y superior.	EXIGIDO	
openSUSE Leap 15.0 y superior.	EXIGIDO	
Ubuntu 20.4 LTS y superior.	EXIGIDO	
La solución EDR con capacidades EPP debe disponer mínimamente los siguientes módulos de protección, control y hardening:	EXIGIDO	
Firewall	EXIGIDO	
AV de Archivos, Web y Mail.	EXIGIDO	
Detección Avanzada ML.	EXIGIDO	
Detección reputación Nube.	EXIGIDO	
Módulo de prevención de ataques de red (IDS)	EXIGIDO	
Prevención de intrusiones en el host (HIPS).	EXIGIDO	
Autoprotección (contra ataques a los servicios/procesos del antivirus)	EXIGIDO	
Control de dispositivos.	EXIGIDO	
Control de acceso a sitios web por categoría.	EXIGIDO	
Control de aplicaciones.	EXIGIDO	
Protección AMSI	EXIGIDO	
Control de vulnerabilidades de Windows y de los aplicativos de terceras partes.	EXIGIDO	
Modulo Anti-Ransomware.	EXIGIDO	

Modulo Prevención de explotación de vulnerabilidades. (AEP).	EXIGIDO	
Cifrado de disco, carpetas y archivos y unidades removibles.	EXIGIDO	
Detección y Respuesta EDR	EXIGIDO	
La solución debe contar con modulo Antivirus web (módulo para verificación de sitios y downloads antivirus) que incluya la auditoria de tráfico HTTP como Trafico HTTPS sin necesidad de instalación de plug-in o componente adicional en el navegador.	EXIGIDO	
La solución debe contar con modulo Antivirus de correo electrónico (módulo para verificación de correos recibidos y enviados, así como sus adjuntos) sin necesidad de instalación de plug-in o componente adicional.	EXIGIDO	
Las firmas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo).	EXIGIDO	
Debe de permitir la integración y escaneo de IOCs.	EXIGIDO	
Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación.	EXIGIDO	
Debe tener módulo que analice las acciones de cada aplicación en ejecución en la computadora, grabando las acciones ejecutadas y comparándolas con secuencias características de actividades peligrosas. Tales registros de secuencias deben ser actualizados conjuntamente con las firmas.	EXIGIDO	
Debe contar con módulo que analice cualquier intento de edición, exclusión o grabación del registro, de forma que sea posible elegir claves específicas para ser monitoreadas y/o bloqueadas.	EXIGIDO	
Debe tener módulo de control que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínimo:	EXIGIDO	
Discos de almacenamiento locales	EXIGIDO	
Almacenamiento extraíble	EXIGIDO	
Impresoras	EXIGIDO	

CD/DVD, Drives de disquete	EXIGIDO	
Modems	EXIGIDO	
Dispositivos de cinta	EXIGIDO	
Lectores de smart card	EXIGIDO	
Dispositivos de sincronización vía ActiveSync (Windows CE, Windows Mobile, etc.)	EXIGIDO	
Wi-Fi	EXIGIDO	
Adaptadores de red externos	EXIGIDO	
Dispositivos MP3 o smartphones	EXIGIDO	
Dispositivos Bluetooth	EXIGIDO	
Capacidad de liberar acceso a un dispositivo específico y usuarios específicos por un período de tiempo específico, sin la necesidad de deshabilitar la protección, sin deshabilitar el gerenciamento central o de intervención local del administrador en la máquina del usuario.	EXIGIDO	
Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por usuario y acorde a un rango horario.	EXIGIDO	
Capacidad de limitar el acceso a sitios de internet por categoría y/o por contenido (video, audio, etc.), con posibilidad de configuración por usuario o grupos de usuarios y agendamiento.	EXIGIDO	
Capacidad de limitar la ejecución de aplicativos por hash MD5, nombre del archivo, versión del archivo, nombre del aplicativo, versión del aplicativo, fabricante/desarrollador, categoría (ej.: navegadores, gestor de descargas, juegos, aplicación de acceso remoto, etc.).	EXIGIDO	
Capacidad de bloquear la ejecución de un aplicativo que esté en almacenamiento externo.	EXIGIDO	
Capacidad de limitar el acceso de los aplicativos a recursos del sistema, como claves de registro y carpetas/archivos del sistema, por categoría, fabricante o nivel de confianza del aplicativo.	EXIGIDO	

Capacidad de, en caso de que la computadora cliente salga de la red corporativa, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.	EXIGIDO	
La solución debe de poseer módulo de control de aplicaciones que permita la generación de reglas de listas blancas y negras acorde a grupos de categorización dinámica de aplicaciones.	EXIGIDO	
La solución debe de poseer módulo de control de aplicaciones que permita la generación de reglas de lista blanca y negra acorde al inventario de aplicaciones detectadas en la organización.	EXIGIDO	
La solución debe de poseer módulo de protección AMSI.	EXIGIDO	
La solución debe de contar con un módulo de control de anomalías dinámico que permita la configuración de reglas acorde al aprendizaje automático, así como la definición de exclusiones por parte de los administradores.	EXIGIDO	
La solución debe de poseer módulo de AEP (Automatic Exploit Prevention), que permita detectar y contener explotación de vulnerabilidades inclusive aquellas de día 0.	EXIGIDO	
La solución debe disponer de mapeo de técnicas y tácticas	EXIGIDO	
La solución debe proporcionar la capacidad de realizar un análisis de la causa raíz y visualizar los datos relacionados con la amenaza/la cadena de ataque a través del gráfico de ejecución de actividades/procesos.	EXIGIDO	
La solución debe proporcionar un mecanismo para automatizar el proceso de caza de amenazas y realizar un análisis retrospectivo de los datos históricos de telemetría (a través de un constructor de consultas flexible, orientación, etc.).	EXIGIDO	
La solución debe tener integrada la funcionalidad de la plataforma de respuesta a incidentes, incluyendo la capacidad de: Agregar alertas y crear un incidente (tanto manual como automáticamente), Asignar un analista dedicado al incidente, Seguir el estado de los incidentes y Comentar, entre otros.	EXIGIDO	
La solución debe ofrecer la posibilidad de fusionar incidentes e investigarlos como un único problema.	EXIGIDO	

La solución debe proporcionar la capacidad de escanear la infraestructura de los puntos finales utilizando Indicadores de Compromiso (al menos en el formato OpenIOC) - se deben soportar tanto las tareas programadas como bajo demanda.	EXIGIDO	
Debe disponer modulo anti ransomware para la detección y contención de ataques del tipo ransomware sobre carpetas compartidas de red.	EXIGIDO	
Debe proporcionar módulo IDS (Intrusion Detection System) y prevención de ataques de red para protección contra port scans y explotación de vulnerabilidades de software. La base de datos de análisis debe actualizarse conjuntamente con las firmas.	EXIGIDO	
Disponer módulo de cifrado de datos, como mínimo, un algoritmo AES con clave de 256 bits en sistemas operativos Windows de Escritorio.	EXIGIDO	
Capacidad de cifrar completamente el disco duro de la máquina, agregando un ambiente de preboot para autenticación del usuario para sistemas operativos Windows de Escritorio.	EXIGIDO	
Capacidad de cifrar unidades extraíbles o portables.	EXIGIDO	
Capacidad de seleccionar carpetas y archivos (por tipo, o extensión) para ser cifradas automáticamente. En esta modalidad, los archivos deben estar accesibles para todas las máquinas gestionadas por la misma consola de manera transparente para los usuarios.	EXIGIDO	
La solución de seguridad debe estar específicamente diseñada para trabajar sobre entornos virtuales VMWare, Hyper-V, Citrix, Proxmox y KVM bajo una Arquitectura que posibilite el correcto rendimiento de los servidores y al mismo tiempo garantizando la seguridad de los mismos.	EXIGIDO	
Debe reducir el uso de recursos tales como CPU, memoria y disco de cada máquina virtual a través de la implementación de un equipo/appliance/entidad u otro método dedicado al escaneo de todas las máquinas virtuales de manera externa.	EXIGIDO	
Debe contar con una técnica que prevenga el escaneo de archivos ya escaneados en alguna otra máquina virtual de tal manera a ahorrar tiempo de procesamiento.	EXIGIDO	
La solución debe de permitir la gestión de la seguridad en servidores tradicionales (físicos) así como servidores virtuales y servidores que se encuentren alojados en a Amazon AWS y Microsoft Azure.	EXIGIDO	

La solución debe de proveer tecnología para el bloqueo de ataques de red, tanto de forma preventiva como reactiva (IDS/IPS) integrándose nativamente con la arquitectura de VMware NSX o sin requerir de componente adicional.	EXIGIDO	
La solución debe de proveer tecnología para el filtrado de contenido Web integrándose nativamente con la arquitectura de VMware NSX o sin necesidad de integración.	EXIGIDO	
Integración con NSX Security policies y NSX Security TAGs.	EXIGIDO	
Alta disponibilidad del componente de seguridad en caso que uno de los Virtual Appliance de Seguridad no esté disponible.	EXIGIDO	
La solución debe de disponer de métodos de optimización para el procesamiento de objetos a nivel del Virtual Appliance de Seguridad.	EXIGIDO	
La solución debe de disponer de una arquitectura de referencia para la integración con proveedores de virtualización de escritorios (VDI).	EXIGIDO	
La solución debe de impactar lo menos posible el rendimiento de en el aprovisionamiento de escritorios virtuales (Entornos VDI).	EXIGIDO	
La solución debe de proporcionar tecnologías Agentless y de Agente liviano para la integración de controles de seguridad en entornos virtualizados VMware.	EXIGIDO	
Plataforma de Concienciación de Usuarios		
La herramienta debe poseer una plataforma autogestionable que permita la elaboración de campañas de concienciación en ciberseguridad para usuarios de la Entidad.	EXIGIDO	
La plataforma de concienciación debe tener la capacidad de automatizar las campañas.	EXIGIDO	
El contenido debe ser estructurado por niveles y temas, con módulos temáticos. Ej.: phishing, contraseñas, correo seguro, navegación segura, redes sociales, etc. y niveles de dificultad progresiva desde básico a avanzado.	EXIGIDO	
Debe tener un enfoque en competencias prácticas, midiendo si el usuario puede aplicar lo aprendido en situaciones reales	EXIGIDO	

Reportes y dashboard avanzados: debe ofrecer métricas claras de rendimiento por usuarios, departamentos o empresa.	EXIGIDO	
Multilingüe: debe ser capaz de crear campañas en diferentes idiomas, incluyendo de forma mandatoria el español.	EXIGIDO	
Cumplimiento normativo y soporte a auditorías: la plataforma debe ayudar a cumplir requisitos normativos como ISO 27001, GDPR, PCI, DSS, entre otras.	EXIGIDO	
Enfoque en reducción de riesgos humanos: la plataforma debe estar alineada con una estrategia de ciberseguridad centrada en el usuario, entendiendo que el error humano es una de las principales amenazas.	EXIGIDO	
Plataforma Anti-Spam Correo Electrónico		
Se debe proveer una plataforma de protección de correos electrónicos que tenga capacidades de Anti-Spam, Anti-Phishing, Anti-Malware, filtrado de archivos adjuntos y filtrado de contenido.	EXIGIDO	
La solución debe inspeccionar en tiempo real el tráfico de correo (Entrada y Salida) para la remoción de todo tipo de amenazas, virus, worms, troyanos y otros tipos de programas maliciosos incluyendo correos indeseados.	EXIGIDO	
La solución debe ser del mismo fabricante de EDR y XDR para que permita su integración de forma nativa con dichas plataformas. No se contemplarán soluciones que no sean del mismo fabricante.	EXIGIDO	
La solución debe ser proporcionada mediante Imagen de Software en formato ISO para el despliegue sobre plataforma virtualizada acorde a modalidad gateway virtual.	EXIGIDO	
La solución debe disponer capacidades de integración con plataforma XDR con el objetivo de proporcionar capacidades avanzadas de detección de amenazas que incluyan la utilización de reglas Yara y procesamiento de correos acorde a módulo de Sandbox on-premise.	EXIGIDO	
La solución debe ser implementada on-premise y debe disponer de una consola Web de gestión centralizada.	EXIGIDO	
Los módulos y/o componentes de la solución deben estar basados en software/appliance de uso específico, con sistema operativo, base de datos y servicios configurados para óptimo rendimiento y segurización por el fabricante de la solución.	EXIGIDO	

La solución debe proveer un procedimiento por el cual se pueda realizar una actualización de todos y cada uno de los dispositivos que la componen, sin la necesidad de realizar un corte de servicio y sin afectar al resto de los componentes	EXIGIDO	
La solución tiene la capacidad de integración con servicios de reputación locales sin la necesidad de enviar datos fuera de la organización.	EXIGIDO	
La solución dispone de capacidades para el desempaquetado y análisis de archivos compuestos como por ejemplo archivos comprimidos.	EXIGIDO	
La solución debe de detectar, bloquear y desinfectar mensajes de correos electrónicos infectados, así como sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.	EXIGIDO	
La solución debe detectar y bloquear mensajes que contengan anexos con macros (Por ejemplo, archivos en formato Microsoft Office con macros), eliminar mensajes o sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.	EXIGIDO	
La solución debe detectar y bloquear mensajes cifrados, eliminar mensajes o sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.	EXIGIDO	
La solución debe disponer de capacidad de filtrado de contenido de los mensajes mínimamente acorde al nombre, tamaño y tipo de anexo, determinando el formato indiferentemente de su extensión, así como eliminar mensajes o sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.	EXIGIDO	
Los mensajes que se encuentran en el backup deben poder ser guardados y descargados, así como reenviados a su destinatario original u otros destinatarios a ser seleccionados.	EXIGIDO	
La solución debe de procesar los mensajes, acorde a las reglas de seguridad estipuladas para los grupos de remitentes y destinatarios.	EXIGIDO	
La solución debe poder validar el remitente acorde a la autenticación del remitente utilizando tecnologías SPF, DKIM y DMARC.	EXIGIDO	
La solución debe poder firmar correos salientes mediante tecnologías DKIM.	EXIGIDO	
La solución debe permitir la inclusión de un mensaje de alerta en el subject del correo en caso que anexos peligrosos o indeseados sean detectados.	EXIGIDO	

La solución debe permitir la definición de listas de correos blancas/negras globales y personales.	EXIGIDO	
La solución debe contar con tecnologías de validación de imágenes y anexos gráficos para la detección de mensajes de Spam.	EXIGIDO	
La solución debe identificar archivos sospechosos, potencialmente peligrosos, protegidos con contraseña, así como objetos que han tenido algún error en su análisis. Los mismos deben ser adicionalmente enviados al módulo de Sandbox para su procesamiento.	EXIGIDO	
La solución debe poder eliminar mensajes o sus anexos para archivos sospechosos, potencialmente peligrosos, protegidos con contraseña, así como objetos que han tenido algún error en su análisis con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.	EXIGIDO	
La solución debe proporcionar capacidades de detección y protección ante ataques del tipo Business Email Compromise (BEC).	EXIGIDO	
La solución debe disponer de tecnologías para la detección de Spam basado en el reconocimiento de dominios spoofed (look-alike).	EXIGIDO	
La solución debe de contar con tecnologías proactivas para la detección de amenazas avanzadas o de día 0.	EXIGIDO	
La solución debe de contar con tecnologías de detección avanzadas para la detección y neutralización de amenazas del tipo ransomware.	EXIGIDO	
En caso de objetos infectados la solución debe poder configurar la realización de las siguientes acciones:	EXIGIDO	
Desinfectar	EXIGIDO	
Eliminar Anexo	EXIGIDO	
Borrar mensaje	EXIGIDO	
Rechazar mensaje	EXIGIDO	
Ignorar	EXIGIDO	

La solución permite la configuración de notificaciones por lo menos a las siguientes direcciones (Administradores, Remitente, Destinatario, adicionales).	EXIGIDO	
La solución debe contar con un sistema de alimentación de contenido por parte del fabricante que proporcione información sobre nuevas amenazas, y bases de reputación. Dicha información debe ser actualizada en forma automática y en tiempo real permitiendo enriquecer el motor de análisis de amenazas de la solución.	EXIGIDO	
La totalidad del análisis y operación de la solución debe realizarse en forma local, solo permitiéndose el envío de hashes cuando sea necesario. La solución no debe enviar ninguna otra información sensible fuera de la institución.	EXIGIDO	
La solución debe disponer soporte para la integración con Microsoft Active Directory y Open LDAP.	EXIGIDO	
La solución incluye el acceso al Backup personal mediante Single Sign-On (SSO) acorde a integración con directorio LDAP.	EXIGIDO	
La solución permite la utilización de expresiones regulares para la composición de reglas de filtrado.	EXIGIDO	
La consola de administración Web, proporciona capacidades de acceso basado en roles y perfiles de usuario. Role Based Access Control (RBAC).	EXIGIDO	
La solución cuenta con capacidades para el envío de eventos a un sistema (SIEM) utilizando protocolo Syslog.	EXIGIDO	
La solución permite la generación de reportes y cuadros de mando acorde al periodo seleccionado (día, semana, mes, año) en formato PDF.	EXIGIDO	
La solución debe proporcionar un cuadro de mando web que incluye como mínimo información de: Estado de la Salud del Sistema, Mensajes Procesados (Entrada/Salida) & Amenazas Detectadas.	EXIGIDO	
La consola Web permite la personalización del cuadro de mando el cual permite configurar múltiples widgets a criterio del administrador de la solución.	EXIGIDO	
La solución debe poder gestionar múltiples dominios de correo electrónico.	EXIGIDO	
La solución debe permitir generar reportes en forma manual o programada a intervalos de tiempo determinados.	EXIGIDO	

Soporte de Monitoreo de la plataforma XDR		
El soporte de monitoreo local debe disponer un modelo 24 horas al día, 7 días a la semana, los 365 días del año, para monitoreo, búsqueda de amenazas, detección de incidentes y una respuesta a incidentes con SLA de reacción inferior a 1 horas para incidentes críticos.	EXIGIDO	
El soporte de monitoreo debe ser brindado de forma directa por el proveedor de las soluciones ofertadas.	EXIGIDO	
Debe de integrarse de manera nativa con la tecnología de XDR propuesta sin requerir instalar componentes o agentes adicionales.	EXIGIDO	
El soporte de monitoreo debe brindar información temprana sobre las amenazas al recibir de manera proactiva los datos proporcionados por el Cliente.	EXIGIDO	
El soporte de monitoreo debe detectar amenazas tanto conocidas como desconocidas.	EXIGIDO	
Se debe proporcionar recomendaciones sobre cómo responder eficazmente a las amenazas detectadas.	EXIGIDO	
Debe ofrecer al menos un período de almacenamiento del historial de incidentes de 180 días.	EXIGIDO	
Debe hacer uso de la tecnología AI/ML en sus algoritmos de detección.	EXIGIDO	
Debe proporcionar alertas de incidentes en tiempo real.	EXIGIDO	
Debe incluir capacidades de respuesta a incidentes tanto gestionados (por el proveedor) como guiados.	EXIGIDO	
Las capacidades administradas por el proveedor deben incluir las siguientes acciones de respuesta mínimamente:	EXIGIDO	
Obtener un archivo	EXIGIDO	
Aislar un equipo	EXIGIDO	
Desactivar el aislamiento de un equipo	EXIGIDO	

Eliminar clave de registro	EXIGIDO	
Permitir un volcado de memoria.	EXIGIDO	
Debe permitir respuestas gestionadas de aceptación/rechazo (por el proveedor).	EXIGIDO	
Debe permitir la comprobación del estado de seguridad y visibilidad de activos.	EXIGIDO	
Debe tener un portal web con paneles que muestren información sobre incidentes, activos y comunicaciones.	EXIGIDO	
Debe admitir un modelo de acceso basado en roles y gestión de roles.	EXIGIDO	
Debe proporcionar mínimamente la siguiente información sobre un incidente:	EXIGIDO	
Estado del incidente	EXIGIDO	
Resumen del incidente	EXIGIDO	
Activos relacionados con el incidente	EXIGIDO	
Tácticas MITRE utilizadas (si corresponde)	EXIGIDO	
Marca de tiempo	EXIGIDO	
IOC basado en activos	EXIGIDO	
IOC basado en red	EXIGIDO	
Descripción técnica completa	EXIGIDO	
Respuestas	EXIGIDO	
Historial de comunicación con el proveedor del soporte	EXIGIDO	
Historial de incidentes.	EXIGIDO	

El soporte de monitoreo debe de clasificar los incidentes de acuerdo a su nivel de gravedad y debe disponer de un SLA para el tiempo de reacción asociado al nivel de gravedad.	EXIGIDO	
Debe permitir enviar notificaciones por correo electrónico y/o mensajería instantánea.	EXIGIDO	
La plataforma que da soporte al soporte debe permitir la creación de informes de incidentes diarios/semanales.	EXIGIDO	
<p>El proveedor deberá disponer o habilitar una sala de monitoreo dentro de las instalaciones del Banco Nacional de Fomento (BNF), en la cual deberán estar asignados de manera presencial y permanente dos (2) técnicos especializados, quienes serán responsables del monitoreo de la solución implementada.</p> <p>El horario de trabajo de dichos técnicos será el establecido por la institución, de lunes a viernes, de 08:00 a 17:00 horas, incluyendo una pausa de una (1) hora para el almuerzo a las 12:00 horas.</p> <p>Los técnicos podrán ser rotados por el proveedor, siempre que se mantenga de forma continua y simultánea la presencia de al menos dos (2) técnicos en la sala de monitoreo durante el horario mencionado y durante todo el periodo de licenciamiento (12 meses).</p>	EXIGIDO	
Soporte Técnico y Certificaciones		
El proveedor de las soluciones ofertadas deberá brindar soporte técnico en sitio y/o remoto, en idioma español, durante el período de licenciamiento de 12 meses, que incluya:	EXIGIDO	
Creación de tickets de soporte ilimitados.	EXIGIDO	
Actualización a la consola de Administración de la solución XDR y todos los componentes asociados.	EXIGIDO	
Actualización de versiones	EXIGIDO	
Respuesta ante incidentes.	EXIGIDO	
Administración de parches de seguridad.	EXIGIDO	
Análisis forense e indicadores de compromisos	EXIGIDO	
Informes semanales de eventos de seguridad.	EXIGIDO	

Implementación de todos los módulos de la herramienta en todo el parque de equipos	EXIGIDO	
El proveedor deberá contar con una plataforma y/o sistema de ticket para atención de casos de soporte técnico, a fin de garantizar la respuesta de manera profesional y organizada.	EXIGIDO	
El proveedor local deberá contar con una plataforma de autoservicio de preguntas frecuentes, con por lo menos 50 plantillas de respuesta para esos casos, dicha plataforma deberá estar integrada con el sistema del ticket del proveedor.	EXIGIDO	
El fabricante del producto deberá impartir capacitación oficial la solución ofertada, la cual debe incluir derecho a examen de certificación.	EXIGIDO	
El personal encargado de realizar la capacitación oficial deberá poseer calificación de Instructores Certificados por el fabricante del software involucrado en la solución propuesta.	EXIGIDO	
La capacitación debe estar homologada como un curso oficial de la solución ofertada y tendrán modalidad teórico-práctico incluyendo no sólo en el conocimiento de la solución adjudicada, sino también en la resolución de los problemas propios de una red con las características de la del presente llamado.	EXIGIDO	
La currícula de capacitación oficial teórica/práctica tendrá una duración mínima de (40) horas on-line y realizada por el fabricante de las soluciones ofertadas.	EXIGIDO	
Los materiales a entregar deberán ser en idiomas español y/o inglés	EXIGIDO	
El curso de capacitación oficial propuesto deberá incluir detalladamente:	EXIGIDO	
Objetivos.	EXIGIDO	
Contenidos.	EXIGIDO	
Perfil mínimo requerido para los participantes.	EXIGIDO	
Duración y frecuencia de las reuniones de transferencia de conocimientos.	EXIGIDO	
Modalidad del dictado y esquema del laboratorio.	EXIGIDO	

Antecedentes (curriculum vitae) del personal a cargo del dictado.	EXIGIDO	
Cronograma del dictado.	EXIGIDO	
Metodología de la evaluación final (si la hubiere).	EXIGIDO	
Para todos los asistentes deberá emitirse certificados oficiales del fabricante, referidos a la asistencia a estas reuniones de transferencia tecnológica.	EXIGIDO	
El proveedor local deberá contar como mínimo con 1 técnico con certificación CEH o CEH MASTER o similar.	EXIGIDO	
El proveedor local deberá contar como mínimo con 2 técnicos certificados con las certificaciones avanzadas del producto de detección y respuesta extendida XDR.	EXIGIDO	
El proveedor local deberá contar como mínimo con 2 técnicos con certificaciones de cifrado.	EXIGIDO	
El proveedor local deberá contar como mínimo con 2 técnicos con certificaciones en protección de servidores de correo antispam.	EXIGIDO	
Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar certificados de inscripción en IPS.	EXIGIDO	
El proveedor local deberá contar con el mayor nivel de certificación/partnership posible la marca ofertada, para garantizar el buen servicio y respaldo del soporte local.	EXIGIDO	
El proveedor local deberá tener la Certificación ISO 9001: Sistema de Gestión de Calidad y la Certificación ISO 27001: Sistema de Gestión de Seguridad de la Información para garantizar el buen servicio y respaldo del soporte local.	EXIGIDO	
El proveedor deberá presentar autorización del fabricante expresamente dirigido a la convocante refiriendo el nro. de ID del llamado.	EXIGIDO	
El fabricante de las soluciones ofertadas debe contar con experiencia probada en el descubrimiento de vulnerabilidades desconocidas, APTs y malware avanzado y debe haber descubierto al menos dos (2) vulnerabilidades agregadas a la lista de Common Vulnerabilities and Exposures (CVE) en los últimos meses.	EXIGIDO	

El fabricante de las soluciones ofertadas debe brindar soporte a través de una página web, email y línea telefónica.

EXIGIDO

De las MIPYMES

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

Plan de entrega de los bienes

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

Ítem N°	Descripción	Cantidad	Unidad de Medida	Lugar de Entrega	Plazo de Entrega
1	ADQUISICIÓN DE LICENCIAMIENTO DE SOFTWARE DE SOPORTE TÉCNICO ANTIVIRUS, conforme a las EETT.	1	Unidad	Independencia Nacional esq. 25 de mayo. Casa Matriz Gerencia Departamental de Seguridad Lógica, BNF.	Una vez firmado el contrato, el oferente tendrá 45 (cuarenta cinco) días corridos para la instalación y puesta en funcionamiento.

Plan de prestación de los servicios

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

No Aplica

Planos y diseños

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

No Aplica

Embalajes y documentos

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

No Aplica

Inspecciones y pruebas

Las inspecciones y pruebas serán como se indica a continuación:

No Aplica

CONDICIONES CONTRACTUALES

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

Interpretación

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

Documentación electrónica

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

Formalización de la contratación

Se formalizará esta contratación mediante:

Contrato

Documentación requerida para la firma del contrato

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

1. Personas Físicas / Jurídicas

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

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

2. Documentos. Consorcios

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

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

Indicadores de Cumplimiento de Contrato

El documento requerido para acreditar el cumplimiento contractual, será:

- Para bienes y Servicios: Acta de recepción
- Serán presentados: 1 (un) Acta de recepción
- Frecuencia: única entrega

Justificación: Se establece una frecuencia distinta a lo establecido en la normativa teniendo en cuenta que se trata de renovación de licencias, una vez activadas se procederá al pago previa emisión de las actas de recepción para cada ítem.

Planificación de indicadores de cumplimiento:

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA
• Acta	• Acta de recepción	Conforme al Plazo de Entrega.

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

de contratación de que se trate, deberá indicar el documento a ser comunicado a través del módulo de Seguimiento de Contratos y la cantidad de los mismos.

Subcontratación

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

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

Derechos Intelectuales

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

2. Sujeto al cumplimiento por parte de la contratante del párrafo siguiente, el proveedor indemnizará y liberará de toda responsabilidad a la contratante, sus empleados y funcionarios en caso de pleitos, acciones o procedimientos administrativos, reclamaciones, demandas, pérdidas, daños, costos y gastos de cualquier naturaleza, incluyendo gastos y honorarios por representación legal, que la contratante tenga que incurrir como resultado de la transgresión o supuesta transgresión de derechos de propiedad intelectual como patentes, dibujos y modelos industriales registrados, marcas registradas, derechos de autor u otro derecho de propiedad intelectual registrado o ya existente en la fecha del contrato debido a:

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

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

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

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

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

6. La contratante deberá indemnizar y eximir de culpa al proveedor y a sus empleados, funcionarios y subcontratistas, por cualquier litigio, acción legal o procedimiento administrativo, reclamo, demanda, pérdida, daño, costo y gasto, de cualquier naturaleza, incluyendo honorarios y gastos de abogado, que pudieran afectar al proveedor como resultado de cualquier

transgresión o supuesta transgresión de patentes, modelos de aparatos, diseños registrados, marcas registradas, derechos de autor, o cualquier otro derecho de propiedad intelectual registrado o ya existente a la fecha del contrato, que pudieran suscitarse con motivo de cualquier diseño, datos, planos, especificaciones, u otros documentos o materiales que hubieran sido suministrados o diseñados por la contratante o a nombre suyo.

Transporte

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

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

No Aplica

Confidencialidad en el procedimiento de contratación y el contrato

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

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

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

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

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

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

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

1. El proveedor deberá proporcionar los datos de identificación de sus subproveedores, así como de las personas físicas por medio de las cuales propone cumplir con las obligaciones del contrato, dentro de los treinta días posteriores a la obtención del código de contratación, y con anterioridad al primer pago que vaya a percibir en el marco de dicho contrato, con las especificaciones respecto a cada una de ellas. A ese respecto, el contratista deberá consignar dichos datos en el Formulario de Identificación del Personal (FIP) y en el Formulario de Identificación de Servicios Personales (FIS), a través del Registro del Proveedor del Estado.
2. Cuando ocurra algún cambio en la nómina del personal o de los subcontratistas propuestos, el proveedor o contratista está obligado a actualizar el FIP.
3. Como requerimiento para efectuar los pagos a los proveedores o contratistas, la contratante, a través del procedimiento establecido para el efecto por la entidad previsional, verificará que el proveedor o contratista se encuentre al día en el cumplimiento con sus obligaciones para con el Instituto de Previsión Social (IPS).
4. La contratante podrá realizar las diligencias que considere necesarias para verificar que la totalidad de las personas que prestan servicios personales en relación de dependencia para la contratista y eventuales subcontratistas se encuentren debidamente individualizados en los listados recibidos.
5. El proveedor o contratista deberá permitir y facilitar los controles de cumplimiento de sus obligaciones de aporte obrero patronal, tanto los que fueran realizados por la contratante como los realizados por el IPS, y por funcionarios de la DNCP. La negativa expresa o tácita se considerará incumplimiento del contrato por causa imputable al proveedor o contratista.
6. En caso de detectarse que el proveedor o contratista o alguno de los subcontratistas, no se encontraran al día con el cumplimiento de sus obligaciones para con el IPS, deberán ser emplazados por la contratante para que en diez (10) días hábiles cumplan con sus obligaciones pendientes con la previsional. En el caso de que no lo hiciera, se considerará incumplimiento del contrato por causa imputable al proveedor o contratista.

Porcentaje de Garantía de Fiel Cumplimiento de Contrato

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

10,00 %

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

Forma de Instrumentación de Garantía de Fiel Cumplimiento de Contrato

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

Periodo de validez de la Garantía de Cumplimiento de Contrato

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

La Garantía de Fiel Cumplimiento de Contrato deberá extenderse por todo el periodo de ejecución del Contrato: Plazo de ejecución de la adquisición: 12 meses, más 1 (un) mes de plazo de liberación de la Garantía de Fiel Cumplimiento de Contrato.

La Garantía de Fiel Cumplimiento de Contrato deberá ser presentada en las oficinas de la GDOC - Casa Matriz del BNF (25 de Mayo casi Yegros).

En circunstancias motivadas, la Contratante solicitará al Proveedor que presente prórrogas extendiendo el periodo de validez de la Garantía de Cumplimiento de Contrato, la cual deberá ser presentada antes del vencimiento. La falta de constitución y entrega oportuna de la prórroga de la garantía podrá ser causal de la Ejecución de la Garantía de Cumplimiento de Contrato, y posterior Rescisión del Contrato por hecho imputable al Proveedor y comunicado a la Dirección de Contrataciones Públicas.

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

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

Formas y condiciones de pago

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

1. Documentos Genéricos:

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

Otras formas y condiciones de pago al proveedor en virtud del contrato serán las siguientes: Plazo de pago: como máximo hasta 60 días calendarios. Los proveedores adjudicados deberán presentar documentos requeridos por la SEPRELAD según el Artículo 33 de la Resolución 70/2019 política de Conozca a su proveedor formulario Anexo 2 Perfil del cliente. Así mismo, se deberá adjuntar al legajo documentario copia de la nota de notificación de adjudicación emitida por la Gerencia Departamental Operativa de Contrataciones.

Conforme al Artículo 63 de la Ley N° 7021/22 De Contrataciones Públicas, se retendrá el 0,4% (cero puntos cuatro por ciento) sobre el importe de cada factura, deducido los impuestos correspondientes, al momento de su cobro.

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

3. De conformidad a las disposiciones del Decreto N° 7781/2006, del 30 de junio de 2006 y modificatoria, en las contrataciones con

Organismos de la Administración Central, el proveedor deberá habilitar su respectiva cuenta corriente o caja de ahorro en un Banco de plaza y comunicar a la Contratante para que ésta gestione ante la Dirección General del Tesoro Público, la habilitación en el Sistema de Tesorería (SITE).

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

Solicitud de suspensión de la ejecución del contrato

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

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

Si la demora en el pago fuese superior a ciento veinte (120) días corridos, el proveedor, consultor o contratista podrá proceder a la suspensión del cumplimiento del contrato, debiendo comunicar a la contratante con un mes de antelación tal circunstancia, a efectos del reconocimiento de los derechos que puedan derivarse de dicha suspensión, en los términos establecidos en la Ley. En este supuesto, el pago total de lo adeudado por la contratante determinará la continuidad del cumplimiento del contrato.

Anticipo MIPYMES

Se otorgará Anticipo MIPYMES:

No Aplica

Solicitud de Pago de Anticipo

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

No Aplica

Forma de Instrumentación de Garantía de anticipo

La forma de instrumentación de la Garantía de Anticipo será:

No Aplica

Reajuste

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

PARA BIENES DE ORIGEN NACIONAL:

EL PROVEEDOR solicitará por escrito a **La contratante** el reajuste de precios exponiendo la causa del mismo.

La contratante reconocerá un reajuste en los costos de los bienes, en la medida en que durante su vigencia, exista una variación sustancial de precios en la economía nacional y ésta se vea reflejada en el índice de los precios de consumo, publicado por el Banco Central del Paraguay, en un valor igual o mayor al 15% (quince) por ciento, referente a la fecha de apertura. Los reajustes se aplicarán de la siguiente manera:

$$Pr = P \times IPC1 / IPC0$$

Donde:

Pr: Precio reajustado.

P: Precio adjudicado.

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

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

PARA BIENES IMPORTADOS

EL PROVEEDOR solicitará por escrito a **La contratante** el reajuste de precios exponiendo la causa del mismo.

La contratante reconocerá un reajuste en los costos de los bienes, en la medida en que durante su vigencia exista variación en función a la fluctuación del Dólar Americano, siempre que esta haya sufrido una variación como mínimo de un 10% desde la fecha de apertura, para ello se aplicará la siguiente fórmula:

$$V1 = P \times ((Cmc / Co) - 1)$$

V1= Reajuste de la Oferta

P= Precio de los Bienes (en la Oferta)

Cmc= Tipo de Cambio Referencial (emitido por el BCP) Guaraníes /Dólar Americano del último día hábil del mes anterior a la presentación de la factura.

Co= Tipo de Cambio Referencial (emitido por el BCP) Guaraníes/ Dólar Americano de 3 (tres) días antes de la apertura de oferta).

Los precios reajustados, solo tendrán incidencia sobre los bienes aún no ejecutados; y, no tendrán ningún efecto retroactivo respecto a los servicios que fueron ejecutados antes de la verificación del reajuste.

Para tal efecto, EL PROVEEDOR deberá solicitar por escrito a LA CONTRATANTE

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

Porcentaje de multas

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

0,50 %

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

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

Tasa de interés por Mora

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

0,08

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

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

Si la contratante no efectuara cualquiera de los pagos al proveedor en las fechas de vencimiento correspondiente, la contratante pagará al proveedor interés sobre los montos de los pagos morosos a la tasa establecida en este apartado, por el período de la demora hasta que haya efectuado el pago completo, ya sea antes o después de cualquier juicio.

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

Impuestos y derechos

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

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

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

No Aplica

Convenios Modificatorios

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

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

Limitación de responsabilidad

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

Responsabilidad del proveedor

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

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.

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, catástrofes naturales, incendios, inundaciones, epidemias, pandemias, restricciones de cuarentena, embargos de cargamentos, explosiones, guerras, insurrección, movilización,

huelgas, temblores de tierras y decisiones gubernamentales.

Para fines de esta cláusula, "Caso Fortuito" significa es un evento extraordinario, imprevisto, inevitable, que imposibilita absolutamente el cumplimiento de la prestación y/u obligación.

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.

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.

Si se produjera un acontecimiento de Caso fortuito o fuerza mayor, el contratista tendrá derecho a una prórroga razonable de los plazos de ejecución.

Si se presentara un evento de Caso Fortuito o de Fuerza Mayor, el proveedor notificará por escrito a la contratante sobre dicha condición y causa, en el plazo de siete (7) días calendario a partir del día siguiente en que el proveedor haya tenido conocimiento del evento o debiera haber tenido conocimiento del evento. Transcurrido el mencionado plazo, sin que el proveedor o contratista haya notificado a la convocante la situación que le impide cumplir con las condiciones contractuales, no podrá invocar caso fortuito o fuerza mayor. Excepcionalmente, la convocante bajo su responsabilidad, podrá aceptar la notificación del evento de caso fortuito o de fuerza mayor en un plazo mayor, debiendo acreditar el interés público comprometido.

El caso fortuito o de fuerza mayor debe ser invocado 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

Causales de terminación del contrato

1. Terminación por Incumplimiento

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

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

2. Terminación por insolvencia o quiebra

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

3. Terminación por conveniencia

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

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

entre las siguientes opciones:

- Que se complete alguna porción y se entregue de acuerdo con las condiciones y precios del contrato; y/o
- Que se cancele la entrega restante y se pague al proveedor una suma convenida por aquellos bienes que hubiesen sido parcialmente completados y por los materiales y repuestos adquiridos previamente por el proveedor.

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

Otras causales de terminación del contrato

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

No Aplica

Medio alternativo de Resolución de Conflictos a través del Avenimiento.

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

Medio Alternativo de Resolución de Conflictos a través de la Mediación

El procedimiento de Mediación se podrá llevar a cabo ante:

No Aplica

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

Medio alternativo de Resolución de Conflictos a través del Arbitraje

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

No Aplica

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.

MODELO DE CONTRATO

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

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

FORMULARIOS

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

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

