
PLIEGO DE BASES Y CONDICIONES

Convocante:

**Administración Nacional de Electricidad (ANDE)
Uoc Ande**

Nombre de la Licitación:

**LP1873-24 ADQUISICIÓN Y ACTUALIZACIÓN DE SOFTWARE DE CIBERSEGURIDAD
(KASPERSKY) A SOLUCIÓN DE DETECCIÓN Y RESPUESTA EXTENDIDA (XDR)**
(versión 1)

ID de Licitación:

458987



Modalidad:

Licitación Pública Nacional

Publicado el:

07/01/2025

*"Pliego para la Adquisición de Bienes y/o Servicios - CONVENCIONAL - Ley N° 7021/22."
Versión 2*

RESUMEN DEL LLAMADO

Datos de la Convocatoria

ID de Licitación:	458987	Nombre de la Licitación:	Lp1873-24 Adquisición y Actualización de Software de Ciberseguridad (KASPERSKY) a Solución de Detección y Respuesta Extendida (XDR)
Convocante:	Administración Nacional de Electricidad (ANDE)	Categoría:	43000000 - Tecnologías de Información, Telecomunicaciones y Radiodifusiones
Unidad de Contratación:	Uoc Ande	Tipo de Procedimiento:	LPN - Licitación Pública Nacional

Etapas y Plazos

Lugar para Realizar Consultas:	A través del SICP de la Dirección Nacional de Contrataciones Públicas	Fecha Límite de Consultas:	20/01/2025 12:00
Lugar de Entrega de Ofertas:	Módulo de Ofertas Electrónicas	Fecha de Entrega de Ofertas:	27/01/2025 09:00
Lugar de Apertura de Ofertas:	Módulo de Ofertas Electrónicas	Fecha de Apertura de Ofertas:	27/01/2025 09:00

Adjudicación y Contrato

Sistema de Adjudicación:	Total	Anticipo:	No se otorgará anticipo
Vigencia del Contrato:			

Datos del Contacto

Nombre:	C.P. Liliana Rocío Ortiz Benítez	Cargo:	Directora de Contrataciones Públicas
Teléfono:	2172947 - 2172118 - 2172061 - 2172364	Correo Electrónico:	dadli@ande.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 (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. El Estado por medio de las actividades de compra de bienes y/o 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.

En este sentido, Paraguay cuenta con una Política de Compras Públicas Sostenibles y una guía práctica para las convocantes y oferentes, a las cuales se deberán de ajustar y que se encuentran disponibles en los siguientes links: <https://www.contrataciones.gov.py/dncp/compras-publicas-sostenibles/plan-de-accion-compras-publicas-sostenibles/> y https://www.contrataciones.gov.py/dncp/guia-practica-de-compras-publicas-sostenibles-para-convocantes/compras_publicas_sostenibles/

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

Aclaración de los documentos de la convocatoria

Todo potencial oferente que necesite alguna aclaración de la convocatoria o del pliego de bases y condiciones, podrá solicitarla a la convocante a través del (SICP) dentro del plazo establecido. Las consultas recibidas deberán ser respondidas por las convocantes y publicadas directamente a través del SICP.

Se prorrogará de forma automática en el SICP, el plazo tope para la realización de consultas cuando la fecha del acto de presentación de ofertas sea modificada.

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, 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 podrá diferirlas, para que sean respondidas conforme con los plazos de respuestas o emisión de adendas. En todos los casos se deberá levantar acta circunstanciada.

Las aclaraciones realizadas durante los procedimientos de contratación no serán consideradas modificaciones a las bases de la contratación.

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

Formato y firma de la oferta

1. El formulario de oferta y la lista de precios serán firmados, física o electrónicamente, según corresponda por el oferente o por las personas debidamente facultadas para firmar en nombre del oferente.
2. No serán descalificadas las ofertas que no hayan sido firmadas en documentos considerados no sustanciales.
3. Los textos entre líneas, tachaduras o palabras superpuestas serán válidos solamente si llevan la firma de la persona que firma la oferta.
4. La falta de foliatura no podrá ser considerada como motivo de descalificación de las ofertas.

Plazo para presentar las ofertas

Las ofertas deberán ser recibidas por la convocante en la fecha y hora que se indican en el SICP.

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

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

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

Oferentes en consorcio

Dos o más interesados podrán unirse temporalmente para presentar una oferta sin crear una persona jurídica distinta y deberán designar a uno de sus integrantes como líder quien suscribirá la oferta y los documentos relativos al procedimiento de contratación. Se deberá realizar el procedimiento de activación del consorcio directamente a través del Registro de Proveedores del Estado.

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 en un mismo lote o ítem, lo que no impide que puedan presentarse individualmente o conformar otro consorcio que participe en diferentes partidas.

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 o en su defecto acompañada de su traducción oficial, realizada por un traductor público matriculado en la República del Paraguay.

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

No Aplica

Precio y formulario de la oferta

El oferente indicará el precio total de su oferta y los precios unitarios de los bienes y/o servicios que se propone suministrar, utilizando para ello el formulario de oferta y lista de precios, disponibles para su descarga a través del SICP, formando ambos un único documento.

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

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

- El precio cotizado deberá ser el mejor precio posible, considerando que en la oferta no se aceptará la inclusión de descuentos de ningún tipo.
- 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 de todos los ítems, con sus precios unitarios y totales correspondientes.
- En el caso del sistema de adjudicación por lotes, el oferente cotizará en la lista de precios uno o más lotes, e indicará todos los ítems del lote ofertado con sus precios unitarios y totales correspondientes. En caso de no cotizar uno o más lotes, los lotes no cotizados no requieren ser incorporados a la planilla de precios.
- En el caso del sistema de adjudicación por ítems, el oferente podrá ofertar por uno o más ítems, en cuyo caso deberá cotizar el precio unitario y total de cada uno o más ítems, los ítems no cotizados no requieren ser incorporados a la planilla de precios.

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

- 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;
- 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
- 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 cobre el proveedor por los bienes y/o servicios suministrados en virtud del contrato no podrá ser diferente a los precios unitarios cotizados en su oferta, excepto por cualquier ajuste previsto en el mismo.

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

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

Abastecimiento simultáneo

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

No Aplica

Moneda de la oferta y pago

La moneda de la oferta y pago será:

Guaraníes

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

Copias de la oferta - CPS

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

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

Cantidad de copias requeridas:

0 copias

Método de presentación de ofertas

El método de presentación de ofertas para esta convocatoria será:

Un sobre

En caso de presentación física, los sobres deberán:

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

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

Si los sobres no están cerrados e identificados como se requiere, la convocante no se responsabilizará en caso de que la oferta se extravíe o sea abierta prematuramente.

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.

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

Cuando la presentación de oferta sea electrónica la misma deberá sujetarse a la Resolución DNCP N° 3800/23.

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

Ofertas Alternativas

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

No Aplica

Periodo de validez de las ofertas

Las ofertas deberán mantenerse válidas (en días corridos) por:

120

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. 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 formas de instrumentación de las garantías dispuestas en el SICP por la Convocante.
2. La Garantía de Mantenimiento de Oferta en caso de oferentes en consorcio 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 líder del consorcio.
 - b. Consorcio con acuerdo de intención de participación en contrato de consorcio: deberán emitir a nombre del líder del consorcio.
3. La Garantía de Mantenimiento de Ofertas podrá ser ejecutada:
 - a. Si el oferente altera las condiciones de su oferta,
 - b. Si el oferente retira su oferta durante el período de validez de ofertas,
 - c. Si no acepta la corrección aritmética del precio de su oferta, en caso de existir, o
 - d. Si el adjudicatario no procede, por causa imputable al mismo a:
 - d.1 Firmar el contrato,
 - d.2 Suministrar los documentos indicados en las bases de la contratación para la firma del contrato,
 - d.3 Suministrar en tiempo y forma la garantía de cumplimiento de contrato,
 - d.4 Cuando se compruebe que las declaraciones juradas presentadas por el oferente adjudicado con su oferta sean falsas,
 - d.5 No se formaliza el consorcio por escritura pública antes de la firma del contrato.
4. En los casos de contratos abiertos las garantías se regirán por lo dispuesto en el Decreto Reglamentario y la reglamentación emitida por la DNCP para el efecto.
5. En caso de instrumentarse las garantías a través de Garantía Bancaria, deberá estar sustancialmente de acuerdo con el formulario incluido en la Sección "Formularios".
6. Las Garantías tanto de Mantenimiento de Oferta, Cumplimiento de Contrato o de Anticipo, sea cual fuere la forma de instrumentación adoptada, deberá ser pagadera ante solicitud escrita de la convocante donde se haga constar el monto reclamado, cuando se tenga acreditada una de las causales de ejecución de la garantía. En estos casos será requisito que previamente el oferente sea notificado del incumplimiento y la intimación de que se hará efectiva la ejecución del monto asegurado.

Periodo de Validez de la Garantía de Mantenimiento de Oferta

El plazo de validez de la Garantía de Mantenimiento de Oferta (en días calendario) será de:

150

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.

Retiro, sustitución y modificación de las ofertas

1. Un oferente podrá retirar, sustituir o modificar su oferta después de presentada mediante el envío de una comunicación por escrito, debidamente firmada por el representante autorizado. La sustitución o modificación correspondiente de la oferta deberá acompañar dicha comunicación por escrito.
2. Todas las comunicaciones deberán ser:
 - a) Presentadas conforme a la forma de presentación e identificación de las ofertas y además los respectivos sobres deberán estar marcados "RETIRO", "SUSTITUCION" o "MODIFICACION";
 - b) Recibidas por la convocante antes del plazo límite establecido para la presentación de las ofertas;Las ofertas cuyo retiro, sustitución o modificación fuere solicitada serán devueltas sin abrir a los oferentes remitentes, durante el acto de apertura de ofertas.
3. Ninguna oferta podrá ser retirada, sustituida o modificada durante el intervalo comprendido entre la fecha límite para presentar ofertas y la expiración del período de validez de las ofertas indicado en el Formulario de Oferta o cualquier extensión si la hubiere, caso contrario, se hará efectiva la Garantía de Mantenimiento de Oferta.
Cuando la presentación de oferta se realice a través del módulo de oferta electrónica la misma deberá sujetarse a la reglamentación vigente

Apertura de ofertas

1. La entidad convocante procederá a la apertura de las ofertas y, en caso de existir notificaciones de retiro, sustitución o modificación de las propuestas, se leerá durante el acto público en presencia de los oferentes o sus representantes según la hora, fecha y lugar previamente establecidos en el SICP.
2. Cuando la presentación de la oferta sea electrónica, el acto de apertura deberá sujetarse a la reglamentación vigente, en la hora y fecha establecida en el SICP.
3. Primero se procederá a verificar los sobres de las ofertas recibidas, marcados como:
 - a) "RETIRO": Se leerán en voz alta y el sobre con la oferta correspondiente no será abierto sino devuelto al oferente remitente. No se permitirá el retiro de ninguna oferta a menos que la comunicación de retiro contenga una autorización válida y sea leída en voz alta en el acto de apertura de las ofertas.
 - b) "SUSTITUCION": Se leerán en voz alta y se intercambiará con la oferta correspondiente que está siendo sustituida; la oferta sustituida no se abrirá y se devolverá al oferente remitente. No se permitirá la sustitución de ninguna oferta a menos que la comunicación de sustitución contenga una autorización válida y sea leída en voz alta en el acto de apertura de las ofertas.
 - c) "MODIFICACION": Se abrirán y leerán en voz alta con la oferta correspondiente. No se permitirá ninguna modificación a las ofertas a menos que la comunicación de modificación contenga una autorización válida y sea leída en voz alta en el acto de apertura de las ofertas. Solamente se considerarán en la evaluación los sobres que se abren y leen en voz alta durante el Acto de Apertura de las Ofertas.
4. Los representantes de los oferentes que participen en la apertura de las ofertas deberán contar con autorización suficiente para suscribir el acta y para revisar los documentos de los demás oferentes, bastando para ello la presentación de una autorización escrita del firmante de la oferta, esta autorización podrá ser incluida en el sobre oferta o ser portada por el representante.
5. Se solicitará a los representantes de los oferentes presentes que firmen el acta. La omisión de la firma por parte de un oferente no invalida el contenido y efecto del acta. Se distribuirá una copia del acta a todos los presentes.
6. Las ofertas sustituidas y modificadas, que no sean abiertas y leídas en voz alta durante el acto de apertura no podrán ser consideradas para la evaluación sin importar las circunstancias y serán devueltas sin abrir a los remitentes.
7. La falta de firma en un documento sustancial, es considerada una omisión sustancial que no podrá ser subsanada en ninguna oportunidad una vez abiertas las ofertas. En cuanto a la garantía de

mantenimiento de oferta deberá estar debidamente extendida.

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

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

Visita al sitio de ejecución del contrato

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

No Aplica

La visita o inspección técnica debe fijarse al menos un (1) día hábil antes de la fecha tope de consulta.

Cuando la convocante haya establecido que será requisito de participación, 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.

En todos los casos, el procedimiento para su realización deberá difundirse en las bases de la contratación.

Las condiciones de participación no deberán ser restrictivas ni limitativas.

Se registrará en acta los asistentes, la fecha, lugar, hora de realización y funcionarios participantes.

Los representantes de los oferentes que asistan 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:

Todos los bienes indicados en la Lista de Precios, en caso de que la empresa oferente no haya fabricado o elaborado el producto ofertado, sino sea importador y/o distribuidor de los bienes, deberá presentar los documentos que demuestren la cadena de autorizaciones desde el fabricante hasta el oferente, vigente y emitida como máximo a la fecha tope de presentación y apertura de ofertas.

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

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

Muestras

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

No Aplica

En caso de ser solicitadas, las muestras deberán ser presentadas junto con la oferta, o bien en el momento y plazo fijado por la convocante en este apartado, la cual será considerada requisito indispensable para la evaluación de la oferta. 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:

Dentro de las veinticuatro (24) horas, contado a partir del reclamo escrito efectuado por la Contratante al Proveedor.

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:

La Garantía por los Bienes suministrados permanecerá vigente durante mil noventa y cinco (1.095) días, contado a partir de la emisión del Certificado de Recepción Provisional correspondiente a dichos bienes conforme al Plan de Entrega establecido.

Cobertura de Seguro de los bienes

La cobertura de seguro requerida a los bienes será:

A cargo del Proveedor.

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

REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN

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

Condición de Participación

Podrán participar de este procedimiento, las personas físicas, jurídicas y/o Consorcio, constituidos o con acuerdo de intención, 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 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.

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 en concordancia con el Artículo 19 de su Decreto Reglamentario. Esta declaración forma parte del formulario de oferta en los casos que el procedimiento de contratación sea convencional y formulario de Oferta electrónica en el caso que se utilice el módulo de oferta electrónica.

Serán desechadas 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, la declaración jurada de no estar comprendido en las prohibiciones y limitaciones para presentar propuesta y contratar, y además las constancias de registro de estructura jurídica y de beneficiarios finales.
2. Verificará los registros del personal de la convocante para detectar si el oferente o sus representantes, se hallan comprendidos en el artículo 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, aparecen en la base de datos del SINARH del VICE MINISTERIO DE CAPITAL HUMANO Y GESTION ORGANIZACIONAL.
4. Si se constata que alguno 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 ejecutar el contrato, 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, 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 g), h), i), y j) de la Ley 7021/22.
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 inhabilitados de la DNCP.
7. Si el Comité confirma que el oferente o sus integrantes poseen impedimentos en virtud a lo dispuesto en el artículo 21 de la Ley N° 7021/22, la oferta será rechazada y se remitirán los antecedentes a la DNCP para los fines pertinentes.

Método de Evaluación

Basado únicamente en precio

Análisis de precios ofertados

La 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:

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

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

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

Para la evaluación de ofertas basada en la multiplicidad de criterios, en cuanto al análisis del precio se podrá considerar el parámetro dispuesto en el presente apartado.

Composición de Precios

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

A continuación, se presenta una estructura para determinar la composición detallada de precios en el marco del Artículo N°4 de la Resolución DNCP N° 454/2024.

ÍTEM	DESCRIPCIÓN DEL BIEN	PRECIO OFERTADO	COSTO DEL BIEN	IMPUESTOS Y CARGAS SOCIALES	GASTOS ADMINISTRATIVOS	RENTABILIDAD
1						
2						

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.

Margen de preferencia en procedimientos de contratación de carácter internacional

En los procedimientos de contratación de carácter internacional, las convocantes otorgarán el beneficio de margen de preferencia del 10% (diez por ciento), a las ofertas que incorporen:

- El empleo de los recursos humanos del país.
- La adquisición y locación de bienes producidos en la República del Paraguay.

Para el otorgamiento del beneficio, los Oferentes deberán acreditar como mínimo el porcentaje de contenido nacional establecido en la reglamentación vigente en la materia.

Requisitos documentales para evaluación de las condiciones de participación.

1. Formulario de Oferta (*)

[El formulario de oferta y lista de precios, generados electrónicamente a través del SICP, deben ser completados y firmados por el oferente.

En caso de que se emplee el módulo de oferta electrónica se considerará que el listado de ítems forma parte del formulario de oferta electrónica, y deberá sujetarse en todo lo demás a la reglamentación vigente.]

2. Garantía de Mantenimiento de Oferta (*)

La garantía de mantenimiento de oferta debe ser extendida, bajo la forma establecida en el SICP.

- Certificado de Cumplimiento con la Seguridad Social (**)
- Certificado de Producto y Empleo Nacional, emitido por el MIC, en caso de contar. (**)
- Certificado de Cumplimiento Tributario. (**)
- Patente comercial del municipio en donde esté asentado el establecimiento del oferente. (**)
- Declaración Jurada de "Declaración de Personas", de conformidad con el formulario estándar - Sección Formularios (*)
- Documentos legales .Oferentes.

8.1. Personas Físicas.

- Fotocopia simple de la Cédula de Identidad del firmante de la oferta. (*)
- Constancia de inscripción en el Registro Único de Contribuyentes – RUC (*)
- En el caso que suscriba la oferta otra persona en su representación, deberá acompañar una fotocopia simple de su cédula de identidad y una fotocopia simple del poder suficiente otorgado por Escritura Pública para presentar la oferta y representarlo en los actos de la licitación. No es necesario que el poder esté inscripto en el Registro de Poderes. (*)

8.2. Personas Jurídicas.

- Fotocopia simple de los documentos que acrediten la existencia legal de la persona jurídica tales como la Escritura Pública de Constitución y protocolización de los Estatutos Sociales. Los estatutos deberán estar inscriptos en la Sección Personas Jurídicas de la Dirección de Registros Públicos. (*)
- Constancia de inscripción en el Registro Único de Contribuyentes. (*)
- Fotocopia simple de los documentos de identidad de los representantes o apoderados de la sociedad. (*)
- 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 otorgado por Escritura Pública (no es necesario que esté inscripto en el Registro de Poderes); o los documentos societarios que justifiquen la representación del firmante, tales como las actas de asamblea y de directorio en el caso de las sociedades anónimas. (*)

8.3. Oferentes en Consorcio.

- Cada integrante del consorcio que sea una persona física domiciliada en la República del Paraguay deberá presentar los documentos requeridos para Oferentes Individuales especificados en el apartado Oferentes Individuales. Personas Físicas. Cada integrante del consorcio que sea una persona jurídica domiciliada en Paraguay deberá presentar los documentos requeridos para Oferentes Individuales Personas Jurídicas. (*)
- Original o fotocopia del consorcio constituido o del acuerdo de intención de constituir el consorcio por escritura pública en caso de resultar adjudicados y antes de la firma del contrato. Las formalidades de los acuerdos de intención y de los consorcios serán determinadas por la Dirección Nacional de Contrataciones Públicas (DNCP). (*)
- Fotocopia simple de los documentos que acrediten las facultades de los firmantes del acuerdo de intención de consorciarse. Estos documentos pueden consistir en(*):
 - Un poder suficiente otorgado por escritura pública por cada miembro del consorcio (no es necesario que esté inscripto en el Registro de Poderes); o
 - Los documentos societarios de cada miembro del consorcio, que justifiquen la representación del firmante, tales como actas de asamblea y de directorio en el caso de las sociedades anónimas.
- Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al consorcio, cuando se haya formalizado el consorcio. Estos documentos pueden consistir en (*):
 - Un poder suficiente otorgado por escritura pública por la Empresa Líder del consorcio (no es necesario que esté inscripto en el Registro de Poderes); o
 - Los documentos societarios de la Empresa Líder, que justifiquen la representación del firmante, tales como actas de asamblea y de directorio en el caso de las sociedades anónimas.

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

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

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

Capacidad Financiera

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

Los mejores tres (3) años de los últimos cuatro (4) años de los ejercicios fiscales cerrados (años 2020, 2021, 2022, 2023).

Para Contribuyentes de IRACIS Y/O IMPUESTO A LA RENTA EMPRESARIAL (IRE): Deberán cumplir con el siguiente parámetro:

- Ratio de Liquidez: activo corriente / pasivo corriente

Deberá ser igual o mayor que 1, en promedio, en los mejores tres (3) años de los últimos cuatro (4) ejercicios fiscales requeridos.

- Endeudamiento: pasivo total / activo total.

No deberá ser mayor a 0,80 en promedio, en los mejores tres (3) años de los últimos cuatro (4) ejercicios fiscales requeridos.

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

El Promedio en los mejores tres (3) años de los últimos cuatro (4) ejercicios fiscales requeridos, no deberá ser negativo.

Para Contribuyentes de IRPC / IRE SIMPLE: Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, en los mejores tres (3) años de los últimos cuatro (4) ejercicios fiscales requeridos.

Para Contribuyentes de IRP: Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso). Deberá ser igual o mayor que 1, en los mejores tres (3) años de los últimos cuatro (4) ejercicios fiscales requeridos.

Para Contribuyentes de exclusivamente IVA General: Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso). Deberá ser igual o mayor que 1, en los mejores tres (3) años de los últimos cuatro (4) ejercicios fiscales requeridos.

En caso de tratarse de un Consorcio, los índices financieros deberán ser cumplidos por cada uno de los integrantes.

La evaluación se realizará aplicando el sistema CUMPLE o NO CUMPLE.

Requisitos documentales para la evaluación de la capacidad financiera

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

a	Fotocopias simples de Balances Generales y Cuadro de Estado de Resultados de los mejores tres (3) años de los últimos cuatro (4) ejercicios fiscales cerrados (2020, 2021, 2022 y 2023) para contribuyentes de IRACIS Y/O IMPUESTO A LA RENTA EMPRESARIAL (IRE). Los mismos deberán estar completos, incluidas todas las notas a los estados financieros y deben corresponder a períodos contables ya completados (no se solicitarán ni aceptarán estados financieros reemplazados se podrá observar en el Registro de Proveedores, el documento correspondiente).
b	Formularios simples de Formularios N° 106 - 501 de los mejores tres (3) años de los últimos cuatro (4) ejercicios fiscales cerrados (2020, 2021, 2022 y 2023) para contribuyentes del IRPC / IRE SIMPLE.
c	Formulario 104 y 515 de los mejores tres (3) años de los últimos cuatro (4) ejercicios fiscales cerrados (2020, 2021, 2022 y 2023) para contribuyentes de Renta Personal - IRP.
d	IVA General de los mejores tres (3) años de los últimos cuatro (4) ejercicios fiscales cerrados (2020, 2021, 2022 y 2023), para contribuyentes sólo del IVA General

Experiencia requerida

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

Demostrar la experiencia en el bien licitado en entidades públicas, privadas y/o mixtas, con facturaciones de venta y/o recepciones finales de contratos ejecutados y finiquitados, por un monto equivalente al cincuenta por ciento (50%) como mínimo del monto total ofertado en la presente licitación, de cualquiera de los tres (3) últimos años (2021, 2022, 2023) o que en la sumatoria totalicen el cincuenta por ciento (50%) del monto total de la Licitación. Pudiendo corresponder los documentos respaldatorios, a cualquiera de los años mencionados hasta verificar el cumplimiento de este requisito. La Convocante sumará el monto indicado en cada documento para verificar el cumplimiento de este requisito.

Para la Experiencia: En caso de tratarse de un Consorcio, se considerará la sumatoria del líder sesenta por ciento (60%) y el socio cuarenta por ciento (40%) de los requisitos establecidos en el punto Experiencia.

La evaluación se realizará aplicando el sistema CUMPLE o NO CUMPLE

Requisitos documentales para la evaluación de la experiencia

1. Copia de facturaciones y/o recepciones finales en entidades públicas, privadas y/o mixtas que avalen la experiencia requerida. Deberán indicarse los datos del contacto de la empresa emisora de la documentación.

Capacidad Técnica

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

Los bienes ofertados deberán satisfacer los requerimientos indicados en las Especificaciones Técnicas.

Se evaluará los datos proporcionados por el Oferente en la Planilla de Datos Garantizados y demás documentos técnicos requeridos en las Especificaciones Técnicas, para determinar si la oferta cumple con las Especificaciones Técnicas que forman parte de los documentos de esta Licitación.

En caso de tratarse de un Consorcio, los requisitos deberán ser cumplidos en su totalidad por al menos 1 (un) integrante del Consorcio.

La evaluación se realizará aplicando el sistema **CUMPLE o NO CUMPLE**

Requisitos documentales para evaluar el criterio de capacidad técnica

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

1. Planilla de Datos Garantizados incluidas en las Especificaciones Técnicas, debidamente llenada y completada. El documento debe ser completado con los datos técnicos y valores en ellas solicitadas. No se admiten referencias a catálogos. Durante la evaluación, la Convocante podrá solicitar aclaraciones dentro de un plazo indicado en el transcurso de la misma. En éste caso, la omisión de algún dato o la aclaración expresamente solicitada será motivo de descalificación.

El Comité de Evaluación podrá solicitar la presentación de la Planilla de Datos Garantizados, debidamente completada en formato editable, en un CD (disco compacto) o pendrive.

Otros criterios que la convocante requiera

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

Luego de la notificación de adjudicación, el proveedor deberá presentar los documentos indicados en el apartado **CONDICIONES CONTRACTUALES EN EL APARTADO DOCUMENTACIÓN REQUERIDA PARA LA FIRMA DEL CONTRATO, LOS MISMOS DEBEN ESTAR VIGENTES A LA FECHA DE FIRMA DEL CONTRATO**.

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.

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.

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

a) Si hay una discrepancia entre un precio unitario y el precio total obtenido al multiplicar ese precio unitario por las cantidades correspondientes, prevalecerá el precio unitario y el precio total será corregido.

b) Si hay un error en un total que corresponde a la suma o resta de subtotales, los subtotales prevalecerán y se corregirá el total.

c) En caso que el oferente haya cotizado su precio en guaraníes con décimos y céntimos la convocante procederá a realizar el redondeo hacia abajo.

Si hay una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras a menos que la cantidad expresada en palabras corresponda a un error aritmético, en cuyo caso prevalecerán

las cantidades en cifras de conformidad con los párrafos (a) y (b) mencionados.

Criterios de desempate de ofertas

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

Criterios de Adjudicación

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

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

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

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

1. La adjudicación en los procedimientos de contratación en los cuales se aplique el atributo de contrato abierto, se efectuará por las cantidades o montos máximos solicitados en el procedimiento de contratación, sin que ello implique obligación de la convocante de requerir la provisión de esa cantidad o monto durante de la vigencia del contrato, obligándose sí respecto de las cantidades o montos mínimos establecidos.
 2. En caso de que la convocante no haya adquirido la cantidad o monto mínimo establecido, deberá consultar al proveedor si desea ampliarlo para el siguiente ejercicio fiscal, hasta cumplir el mínimo.
 3. Al momento de adjudicar el contrato, la convocante se reserva el derecho a disminuir la cantidad de Bienes y/o Servicios requeridos, por razones de disponibilidad presupuestaria u otras razones debidamente justificadas. Estas variaciones no podrán alterar los precios unitarios u otros términos y condiciones de la oferta y de los documentos de la licitación.
- En aquellos procedimientos de contratación en los cuales se aplique el atributo de contrato abierto, cuando la Convocante deba disminuir cantidades o montos a ser adjudicados, no podrá modificar el monto o las cantidades mínimas establecidas en las bases de la contratación.

Notificaciones

Cuando la convocante opte por notificar la adjudicación a través del SICP, la notificación de la misma será realizada de manera automática, 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. La notificación comprenderá la Resolución de la adjudicación, el informe de evaluación.

En sustitución de la notificación a través del SICP, las Convocantes podrán dar a conocer la adjudicación por medios físicos o electrónicos a cada uno de los oferentes, acompañados de la copia íntegra de la resolución de adjudicación y del informe de evaluación, de conformidad al artículo 62 del Decreto.

La no entrega del informe en ocasión de la notificación, suspende el plazo para formular protestas hasta tanto la convocante haga entrega de dicha copia al oferente solicitante.

3. En caso de que la convocante opte por la notificación física a los oferentes participantes, deberá realizarse únicamente con el acuse de recibo y en el mismo con expresa mención de haber recibido el informe de evaluación y la resolución de adjudicación.

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

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

Audiencia Informativa

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

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

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

SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS

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

Suministros y Especificaciones técnicas

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

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

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

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:

1. El Lic. Giancarlo Valentin González Brites, Jefe del Departamento de Tecnología Informática (DTE/DTI), solicita el llamado a Licitación Pública Nacional.
2. El presente pedido no se encuentra previsto en el Programa Anual de Contrataciones (PAC) y obedece a la necesidad de poder garantizar la continuidad del negocio con la segurización de los distintos equipos corporativos de la Institución.
3. Se trata de un llamado sucesivo a fin de garantizar la actualización de Software de Ciberseguridad (Kaspersky) a solución de Detección y Respuesta Extendida (XDR).
4. El objeto de las Especificaciones Técnicas es la de establecer las condiciones mínimas a ser cumplidas para la obtención de la adquisición y actualización de software de ciberseguridad (KASPERSKY) a solución de Detección y Respuesta Extendida (XDR).

Especificaciones técnicas - CPS

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

PLANILLA DE ESPECIFICACIONES TÉCNICAS Y DATOS GARANTIZADOS - N° 19052020-1

ADQUISICIÓN Y ACTUALIZACIÓN DE SOFTWARE DE CIBERSEGURIDAD (KASPERSKY) A SOLUCIÓN DE DETECCIÓN Y RESPUESTA EXTENDIDA (XDR).

Objeto: El objeto de estas especificaciones es la adquisición/actualización y soporte de las licencias de Software de Ciberseguridad (Antivirus) Kaspersky que la Entidad tiene actualmente instaladas y registradas a favor de Administración Nacional de Electricidad.

Las licencias comprenden una suite de soluciones de seguridad principalmente para Estaciones de Trabajo, Buzones de Correo Corporativo, dispositivos móviles y aplicaciones.

De las especificaciones técnicas obligatorias: El proveedor deberá especificar concretamente en su propuesta para el objeto las siguientes especificaciones técnicas. Además de completar obligatoriamente La Planilla de Datos Garantizados que se provee.

Plataforma de Detección y Respuesta Extendida XDR: Exigido.

1. 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.**
2. 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.**
3. 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.**
4. 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.**
5. La solución debe incluir, al menos, las siguientes capacidades de detección: **Exigido.**
 - 5.1. Herramientas de búsqueda de amenazas para buscar de forma proactiva amenazas y vulnerabilidades mediante el análisis de eventos: **Exigido.**
 - 5.2. Detección avanzada de amenazas y correlación cruzada: correlación en tiempo real de eventos de diferentes fuentes: **Exigido.**
 - 5.3. Un gráfico de investigación para visualizar y facilitar la investigación de un incidente e identificar las causas fundamentales de la alerta: **Exigido.**
 - 5.4. 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.**
6. 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.**
7. Como acciones de respuesta la solución debe incluir mínimamente: **Exigido.**
 - 7.1. Acciones de respuesta manuales: aislamiento de endpoints, ejecución de comandos, creación de reglas de prevención y lanzamiento de tareas en un endpoint: **Exigido.**
 - 7.2. Playbooks, tanto predefinidos como creados por el usuario, para automatizar operaciones de respuesta típicas: **Exigido.**
 - 7.3. Acciones de respuesta de productos de terceros y escenarios de respuesta entre productos: **Exigido.**
8. 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.**
 - 8.1. Ejecución remota de tareas de escaneo y actualización: **Exigido.**
 - 8.2. Obtención de información detallada sobre la protección de activos: **Exigido.**
 - 8.3. Configuración de todos los componentes de seguridad a nivel endpoint: **Exigido.**

9. 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**.
10. La solución debe permitir la agrupación de diferentes alertas de múltiples fuentes en un único incidente, para facilitar su gestión e investigación: **Exigido**.
11. 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**.
12. La solución debe disponer de, al menos, 150 integraciones de forma nativa mediante conectores out-of-the-box (predefinidos): **Exigido**.
13. 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**.
14. 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**.
15. La solución debe proporcionar una API abierta, que permita la implementación de escenarios de integración personalizados en la plataforma: **Exigido**.
16. La solución de XDR debe disponer de una consola de gestión con el cien por ciento (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**.
17. 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**.
18. 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**.
19. 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**.
20. 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**.
21. Debe utilizar una red de inteligencia de amenazas y debe disponer de acceso a una base de reputación: **Exigido**.
22. 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**.
- 22.1. Capacidades nocivas de la amenaza: comportamiento malicioso, cambios realizados al sistema operativo, identificación de comandos raw asociados al software malicioso: **Exigido**.
- 22.2. 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**.
- 22.3. Punto de acceso que genere la infección: **Exigido**.
- 22.4. 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**.
23. 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**.
24. 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 cien (100) días: **Exigido**.
25. 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**.
26. 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 treinta (30) palabras: **Exigido**.
27. 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**.
28. 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**.
29. 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**.
30. El proceso de detección de malware del entorno virtual deberá ser capaz de efectuar: **Exigido**.
- 30.1. Análisis dinámico de comportamiento: **Exigido**.
- 30.2. Análisis de patrones y firmas: **Exigido**.
- 30.3. Detección de malware de tipo día cero: **Exigido**.
31. Debe poder identificar comunicaciones que pudieran ser relacionadas con llamadas de comando y control: **Exigido**.
32. 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**.
- 32.1. Registro de Windows: **Exigido**.
- 32.2. Registro de la aplicación: **Exigido**.
- 32.3. Registro de procesos: **Exigido**.
- 32.4. Registro de archivos: **Exigido**.
- 32.5. Registro de comportamiento: **Exigido**.
- 32.6. Registro de comunicaciones: **Exigido**.
33. 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**.
34. 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**.
35. 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**.
36. 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**.
37. 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**.
38. La plataforma de Sandbox facilitará 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**.
39. La plataforma de Sandbox proporcionará información en detalle de la actividad de una muestra dentro de la máquina virtual: **Exigido**.
40. 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**.
41. 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**.
42. 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**.
43. 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**.
44. 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**.
- 44.1. Fecha y hora del ataque: **Exigido**.
- 44.2. Hash MD5/SHA-256. de los binarios maliciosos: **Exigido**.

44.3. Tipo de archivo malicioso detectado: **Exigido.**

44.4. URL/IP de infección: **Exigido.**

44.5. Capacidades nocivas de la amenaza: capacidades de robo de información, comportamiento malicioso, cambios al sistema operativo: **Exigido.**

44.6. Guardar una copia del malware: **Exigido.**

45. 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.**

46. 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.**

Componente EDR con capacidades EPP:

1. 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.**

2. 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.**

3. 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.**

4. La solución debe de poseer servicio de clustering nativo: **Exigido.**

5. 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.**

6. 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.**

7. Debe gestionar estaciones de trabajo y servidores tanto Windows, Linux y macOS, así como dispositivos móviles Android y iOS: **Exigido.**

8. Debe poder realizar la distribución remota de cualquier software, o sea, debe ser capaz de remotamente enviar cualquier software por la estructura de gerenciamento 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.**

9. Debe aplicar actualizaciones y parches de Windows y de terceras partes remotamente en las estaciones de trabajo y servidores: **Exigido.**

10. 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.**

11. 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.**

12. La solución de seguridad para servidores y escritorios debe de proporcionar soporte a OS Windows como Linux: **Exigido.**

13. 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.**

14. 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.**

15. 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.**

16. Debe proporcionar las siguientes informaciones de las computadoras: **Exigido.**

16.1. Si el antivirus está instalado: **Exigido.**

16.2. Si el antivirus ha iniciado: **Exigido.**

16.3. Si el antivirus está actualizado: **Exigido.**

16.4. Minutos/horas desde la última conexión de la máquina con el servidor administrativo: **Exigido.**

16.5. Minutos/horas desde la última actualización de firmas: **Exigido.**

16.6. Fecha y horario de la última verificación ejecutada en la máquina: **Exigido.**

16.7. Versión del antivirus instalado en la máquina: **Exigido.**

16.8. Si es necesario reiniciar la computadora para aplicar cambios: **Exigido.**

16.9. Fecha y horario de cuando la máquina fue encendida: **Exigido.**

16.10. Cantidad de virus encontrados (contador) en la máquina: **Exigido.**

16.11. Nombre de la computadora: **Exigido.**

16.12. Dominio o grupo de trabajo de la computadora: **Exigido.**

16.13. Fecha y horario de la última actualización de firmas: **Exigido.**

16.14. Sistema operativo con Service Pack: **Exigido.**

16.15. Cantidad de procesadores: **Exigido.**

16.16. Cantidad de memoria RAM: **Exigido.**

16.17. Usuario(s) conectados en ese momento, con información de contacto (si están disponibles en el Active Directory): **Exigido.**

16.18. Dirección IP: **Exigido.**

16.19. Aplicativos instalados, inclusive aplicativos de terceros, con historial de instalación, conteniendo fecha y hora que el software fue instalado o removido: **Exigido.**

16.20. Actualizaciones de Windows Updates instaladas: **Exigido.**

16.21. 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.**

16.22. Vulnerabilidades de aplicativos instalados en la máquina: **Exigido.**

17. Debe permitir bloquear las configuraciones del antivirus instalado en las estaciones y servidores de manera que el usuario no consiga modificarlas: **Exigido.**

18. Debe reconectar máquinas clientes al servidor administrativo más próximo, basado en reglas de conexión como: **Exigido.**

18.1. Cambio de Gateway: **Exigido.**

18.2. Cambio de subnet DNS: **Exigido.**

18.3. Cambio de dominio: **Exigido.**

18.4. Cambio de servidor DHCP: **Exigido.**

18.5. Cambio de servidor DNS: **Exigido.**

18.6. Cambio de servidor WINS: **Exigido.**

18.7. Aparición de nueva subnet: **Exigido.**

19. Debe configurar políticas móviles para que cuando una computadora cliente esté fuera de la estructura de protección pueda actualizarse y gestionarse vía internet: **Exigido.**

20. Debe poder realizar la herencia de tareas y políticas en la estructura jerárquica de servidores administrativos: **Exigido.**

21. 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.**

22. Debe exportar informes para los siguientes tipos de archivos: PDF, HTML. y XML: **Exigido.**
23. Debe enviar correos electrónicos para cuentas específicas en caso de algún evento, así como traps SNMP para el monitoreo de eventos **Exigido.**
24. 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.**
25. Debe realizar actualización incremental de firmas en las computadoras clientes: **Exigido.**
26. Debe realizar inventario de hardware y software de todas las máquinas clientes: **Exigido.**
27. La solución deberá ser capaz de detectar amenazas de día cero (zero-day malware) y Amenazas Persistentes Avanzadas (APT): **Exigido.**
28. La solución permitirá la monitorización y captura de eventos de red relacionados a las actividades en PCs y servidores: **Exigido.**
29. 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.**
30. 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.**
31. La solución debe poder tomar entradas para indicadores personalizados de compromiso en formato IOC: **Exigido.**
32. 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.**
33. 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.**
34. 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.**
35. La solución debe ser capaz de proporcionar datos forenses detallados del objeto malicioso adjunto. Los datos forenses deben incluir, entre otros **Exigido.**
- 35.1. Binarios de malware asociado: **Exigido.**
- 35.2. Cualquier cambio en el sistema operativo host: **Exigido.**
- 35.3. Cualquier cambio a la memoria: **Exigido.**
- 35.4. Cualquier cambio en el sistema de archivos: **Exigido.**
- 35.5. Cualquier cambio a la puesta en marcha del sistema: **Exigido.**
36. La solución debe permitir incluir IOCs en lista negra privada de inteligencia bajo formato MD5 / SHA256: **Exigido.**
37. 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.**
38. 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.**
39. La solución debe ser capaz de integrarse con plataformas de SIEM para la administración de logs: **Exigido.**
40. 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.**
41. 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.**
42. 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.**
43. 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.**
44. 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.**
45. La solución debe ser capaz de detectar el ataque localmente, sin depender de un servicio en la nube **Exigido.**
46. Las capacidades de respuesta deben de incluir aislamiento de los equipos afectados acorde a reglas personalizables **Exigido.**
47. La solución debe contar con gateway de conexión para gestión centralizada on-premise de equipos que se encuentren fuera de la red corporativa: **Exigido.**
48. 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.**
49. La solución debe de disponer compatibilidad mínimamente con los siguientes sistemas operativos **Exigido.**
- 49.1. Windows 7 SP1 y superior: **Exigido.**
- 49.2. Windows 8: **Exigido.**
- 49.3. Windows 8.1: **Exigido.**
- 49.4. Windows 10: **Exigido.**
- 49.5. Windows 11: **Exigido.**
- 49.6. MacOS 11.14 o superior: **Exigido.**
- 49.7. Microsoft Windows Server 2008 SP1: **Exigido.**
- 49.8. Microsoft Windows Server 2012 y 2012 R2: **Exigido.**
- 49.9. Microsoft Windows Server 2016: **Exigido.**
- 49.10. Microsoft Windows Server 2019: **Exigido.**
- 49.11. Microsoft Windows Server 2022: **Exigido.**
- 49.12. CentOS 6.7 y superior: **Exigido.**
- 49.13. Debian GNU / Linux 10.1 y superior: **Exigido.**
- 49.14. Linux Mint 19.2 y superior: **Exigido.**
- 49.15. Red Hat Enterprise Linux 6.7 y superior: **Exigido.**
- 49.16. OpenSUSE Leap 15.0 y superior: **Exigido.**
- 49.17. Ubuntu 20.4 LTS y superior: **Exigido.**
50. La solución EDR con capacidades EPP debe disponer mínimamente los siguientes módulos de protección, control y hardening **Exigido.**
- 50.1. Firewall: **Exigido.**
- 50.2. AV de Archivos, Web y Mail: **Exigido.**
- 50.3. Detección Avanzada ML: **Exigido.**
- 50.4. Detección reputación Nube: **Exigido.**
- 50.5. Módulo de prevención de ataques de red (IDS): **Exigido.**
- 50.6. Prevención de intrusiones en el host (HIPS): **Exigido.**
- 50.7. Autoprotección (contra ataques a los servicios/procesos del antivirus): **Exigido.**
- 50.8. Control de dispositivos: **Exigido.**
- 50.9. Control de acceso a sitios web por categoría: **Exigido.**
- 50.10. Control de aplicaciones: **Exigido.**

- 50.11. Protección AMSI: **Exigido**.
- 50.12. Control de vulnerabilidades de Windows y de los aplicativos de terceras partes: **Exigido**.
- 50.13. Modulo Anti-Ransomware: **Exigido**.
- 50.14. Modulo Prevención de explotación de vulnerabilidades (AEP): **Exigido**.
- 50.15. Cifrado de disco, carpetas y archivos y unidades removibles: **Exigido**.
- 50.16. Detección y Respuesta EDR: **Exigido**.
51. 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**.
52. 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**.
53. 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**.
54. Debe de permitir la integración y escaneo de IOC's: **Exigido**.
55. Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación: **Exigido**.
56. 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**.
57. 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**.
58. Debe tener módulo de control que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínima: **Exigido**.
- 58.1. Discos de almacenamiento locales: **Exigido**.
- 58.2. Almacenamiento extraíble: **Exigido**.
- 58.3. Impresoras: **Exigido**.
- 58.4. CD/DVD, Drives de disquete: **Exigido**.
- 58.5. Modems: **Exigido**.
- 58.6. Dispositivos de cinta: **Exigido**.
- 58.7. Lectores de smart card: **Exigido**.
- 58.8. Dispositivos de sincronización vía ActiveSync (Windows CE, Windows Mobile, etc.): **Exigido**.
- 58.9. Wi-Fi: **Exigido**.
- 58.10. Adaptadores de red externos: **Exigido**.
- 58.11. Dispositivos MP3 o smartphones: **Exigido**.
- 58.12. Dispositivos Bluetooth: **Exigido**.
59. 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 gerenciamiento central o de intervención local del administrador en la máquina del usuario: **Exigido**.
60. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por usuario y acorde a un rango horario: **Exigido**.
61. 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**.
62. 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, juego65s, aplicación de acceso remoto, etc.): **Exigido**.
63. Capacidad de bloquear la ejecución de un aplicativo que esté en almacenamiento externo: **Exigido**.
64. 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**.
65. 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**.
66. 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**.
67. 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**.
68. La solución debe de poseer módulo de protección AMSI: **Exigido**.
69. 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**.
70. 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**.
71. La solución debe disponer de mapeo de técnicas y tácticas: **Exigido**.
72. 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**.
73. 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**.
74. 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**.
75. La solución debe ofrecer la posibilidad de fusionar incidentes e investigarlos como un único problema: **Exigido**.
76. 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**.
77. Debe disponer modulo anti ransomware para la detección y contención de ataques del tipo ransomware sobre carpetas compartidas de red: **Exigido**.
78. 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**.
79. Disponer módulo de cifrado de datos, como mínimo, un algoritmo AES con clave de 256 bits en sistemas operativos Windows de Escritorio: **Exigido**.
80. 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**.
81. Capacidad de cifrar unidades extraíbles o portables: **Exigido**.
82. 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**.
83. 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**.
84. 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**.
85. 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**.
86. 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 Amazon AWS y Microsoft Azure: **Exigido**.
87. 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**.

88. 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**.

89. Integración con NSX Security policies y NSX Security TAGs: **Exigido**.

90. Alta disponibilidad del componente de seguridad en caso que uno de los Virtual Appliance de Seguridad no esté disponible: **Exigido**.

91. La solución debe de disponer de métodos de optimización para el procesamiento de objetos a nivel del Virtual Appliance de Seguridad: **Exigido**.

92. La solución debe de disponer de una arquitectura de referencia para la integración con proveedores de virtualización de escritorios (VDI): **Exigido**.

93. La solución debe de impactar lo menos posible el rendimiento de en el aprovisionamiento de escritorios virtuales (Entornos VDI): **Exigido**.

94. La solución debe de proporcionar tecnologías Agentless y de Agente liviano para la integración de controles de seguridad en entornos virtualizados VMware: **Exigido**.

Plataforma Anti-Spam Correo Electrónico:

1. 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**.

2. 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**.

3. 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**.

4. La solución debe ser proporcionada mediante Imagen de Software en formato ISO para el despliegue sobre plataforma virtualizada acorde a modalidad gateway virtual: **Exigido**.

5. 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**.

6. La solución debe ser implementada on-premise y debe disponer de una consola Web de gestión centralizada: **Exigido**.

7. 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 segregación por el fabricante de la solución: **Exigido**.

8. 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**.

9. La solución tiene la capacidad de integración con servicios de reputación locales sin la necesidad de enviar datos fuera de la organización: **Exigido**.

10. La solución dispone de capacidades para el desempaqueado y análisis de archivos compuestos como por ejemplo archivos comprimidos: **Exigido**.

11. 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**.

12. 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**.

13. 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**.

14. 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**.

15. 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**.

16. La solución debe de procesar los mensajes, acorde a las reglas de seguridad estipuladas para los grupos de remitentes y destinatarios: **Exigido**.

17. La solución debe poder validar el remitente acorde a la autenticación del remitente utilizando tecnologías SPF, DKIM y DMARC: **Exigido**.

18. La solución debe poder firmar correos salientes mediante tecnologías DKIM: **Exigido**.

19. 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**.

20. La solución debe permitir la definición de listas de correos blancas/negras globales y personales: **Exigido**.

21. La solución debe contar con tecnologías de validación de imágenes y anexos gráficos para la detección de mensajes de Spam: **Exigido**.

22. 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**.

23. 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**.

24. La solución debe proporcionar capacidades de detección y protección ante ataques del tipo Business Email Compromise (BEC): **Exigido**.

25. La solución debe disponer de tecnologías para la detección de Spam basado en el reconocimiento de dominios spoofed (look-alike): **Exigido**.

26. La solución debe de contar con tecnologías proactivas para la detección de amenazas avanzadas o de día 0: **Exigido**.

27. La solución debe de contar con tecnologías de detección avanzadas para la detección y neutralización de amenazas del tipo ransomware: **Exigido**.

28. En caso de objetos infectados la solución debe poder configurar la realización de las siguientes acciones: **Exigido**.

28.1. Desinfectar: **Exigido**.

28.2. Eliminar Anexo: **Exigido**.

28.3. Borrar mensaje: **Exigido**.

28.4. Rechazar mensaje: **Exigido**.

28.5. Ignorar: **Exigido**.

29. La solución permite la configuración de notificaciones por lo menos a las siguientes direcciones (Administradores, Remitente, Destinatario, adicionales): **Exigido**.

30. 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**.

31. 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**.

32. La solución debe disponer soporte para la integración con Microsoft Active Directory y Open LDAP: **Exigido**.

33. La solución incluye el acceso al Backup personal mediante Single Sign-On (SSO) acorde a integración con directorio LDAP: **Exigido**.

34. La solución permite la utilización de expresiones regulares para la composición de reglas de filtrado: **Exigido**.

35. La consola de administración Web, proporciona capacidades de acceso basado en roles y perfiles de usuario. Role Based Access Control (RBAC): **Exigido**.

36. La solución cuenta con capacidades para en envío de eventos a un sistema (SIEM) utilizando protocolo Syslog: **Exigido**.

37. La solución permite la generación de reportes y cuadros de mando acorde al periodo seleccionado (día, semana, mes, año) en formato PDF: **Exigido**.

38. 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**.

39. La consola Web permite la personalización del cuadro de mando el cual permite configurar múltiples widgets a criterio del administrador de la solución: **Exigido**.

40. La solución debe poder gestionar múltiples dominios de correo electrónico: **Exigido**.

41. La solución debe permitir generar reportes en forma manual o programada a intervalos de tiempo determinados: **Exigido**.

Soporte de Monitoreo de la plataforma XDR:

1. El soporte de monitoreo 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**.

2. El soporte de monitoreo debe ser brindado de forma directa por el fabricante de las soluciones ofertadas: **Exigido**.

3. Debe de integrarse de manera nativa con la tecnología de XDR propuesta sin requerir instalar componentes o agentes adicionales: **Exigido**.

4. El soporte de monitoreo debe brindar información temprana sobre las amenazas al recibir de manera proactiva los datos proporcionados por el Cliente **Exigido**.
 5. El soporte de monitoreo debe detectar amenazas tanto conocidas como desconocidas **Exigido**.
 6. Se debe proporcionar recomendaciones sobre cómo responder eficazmente a las amenazas detectadas **Exigido**.
 7. Debe ofrecer al menos un período de almacenamiento del historial de incidentes de 1 año **Exigido**.
 8. Debe hacer uso de la tecnología AI/ML en sus algoritmos de detección **Exigido**.
 9. Debe proporcionar alertas de incidentes en tiempo real **Exigido**.
 10. Debe incluir capacidades de respuesta a incidentes tanto gestionados (por el proveedor) como guiados **Exigido**.
 11. Las capacidades administradas por el proveedor deben incluir las siguientes acciones de respuesta mínimamente **Exigido**.
 - 11.1. Obtener un archivo: **Exigido**.
 - 11.2. Aislar un equipo: **Exigido**.
 - 11.3. Desactivar el aislamiento de un equipo: **Exigido**.
 - 11.4. Eliminar clave de registro: **Exigido**.
 - 11.5. Permitir un volcado de memoria: **Exigido**.
 12. Debe permitir respuestas gestionadas de aceptación/rechazo (por el proveedor): **Exigido**.
 13. Debe permitir la comprobación del estado de seguridad y visibilidad de activos **Exigido**.
 14. Debe tener un portal web con paneles que muestren información sobre incidentes, activos y comunicaciones **Exigido**.
 15. Debe admitir un modelo de acceso basado en roles y gestión de roles **Exigido**.
 16. Debe proporcionar mínimamente la siguiente información sobre un incidente: **Exigido**.
 - 16.1. Estado del incidente: **Exigido**.
 - 16.2. Resumen del incidente: **Exigido**.
 - 16.3. Activos relacionados con el incidente: **Exigido**.
 - 16.4. Tácticas MITRE utilizadas (si corresponde): **Exigido**.
 - 16.5. Marca de tiempo: **Exigido**.
 - 16.6. IOC basado en activos: **Exigido**.
 - 16.7. IOC basado en red: **Exigido**.
 - 16.8. Descripción técnica completa: **Exigido**.
 - 16.9. Respuestas: **Exigido**.
 - 16.10. Historial de comunicación con el proveedor del soporte: **Exigido**.
 - 16.11. Historial de incidentes: **Exigido**.
 17. 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**.
 18. Debe permitir enviar notificaciones por correo electrónico y/o mensajería instantánea: **Exigido**.
 19. La plataforma que da soporte al soporte debe permitir la creación de informes de incidentes diarios/semanales: **Exigido**.
- Soporte Técnico y Certificaciones:**
1. El fabricante de las soluciones ofertadas deberá brindar soporte técnico en sitio y/o remoto, en idioma español e inglés, 24/7 con un mínimo de 320 horas garantizadas durante el período de licenciamiento de 36 meses, que incluya: **Exigido**.
 - 1.1. Creación de tickets de soporte ilimitados: **Exigido**.
 - 1.2. Actualización a la consola de Administración de la solución XDR y todos los componentes asociados: **Exigido**.
 - 1.3. Actualización de versiones: **Exigido**.
 - 1.4. Respuesta ante incidentes: **Exigido**.
 - 1.5. Administración de parches de seguridad: **Exigido**.
 - 1.6. Análisis forense e indicadores de compromisos: **Exigido**.
 - 1.7. Informes semanales de eventos de seguridad: **Exigido**.
 - 1.8. Implementación de todos los módulos de la herramienta en todo el parque de equipos: **Exigido**.
 2. El soporte del fabricante de las tecnologías consideradas debe incluir un Gerente de Cuenta Técnica (TAM) dedicado exclusivamente para **ANDE** y que permita la resolución proactiva de problemas y reuniones frecuentes de seguimiento: **Exigido**.
 3. 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**.
 4. 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**.
 5. El fabricante del producto deberá impartir capacitación oficial la solución ofertada, la cual debe incluir derecho a examen de certificación: **Exigido**.
 6. 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**.
 7. 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**.
 8. La currícula de capacitación oficial teórica/práctica tendrá una duración mínima de (40) horas on-site y realizada por el fabricante de soluciones ofertadas **Exigido**.
 9. Los materiales a entregar deberán ser en idiomas español y/o inglés: **Exigido**.
 10. El curso de capacitación oficial propuesto deberá incluir detalladamente: **Exigido**.
 - 10.1. Objetivos: **Exigido**.
 - 10.2. Contenidos: **Exigido**.
 - 10.3. Perfil mínimo requerido para los participantes: **Exigido**.
 - 10.4. Duración y frecuencia de las reuniones de transferencia de conocimientos: **Exigido**.
 - 10.5. Modalidad del dictado y esquema del laboratorio: **Exigido**.
 - 10.6. Antecedentes (curriculum vitae) del personal a cargo del dictado: **Exigido**.
 - 10.7. Cronograma del dictado: **Exigido**.
 - 10.8. Metodología de la evaluación final (si la hubiere): **Exigido**.
 11. Para todos los asistentes deberá emitirse certificados oficiales del fabricante, referidos a la asistencia a estas reuniones de transferencia tecnológica: **Exigido**.
 12. El proveedor local deberá contar como mínimo con 1 técnico con certificación CEH o CEH MASTER o similar.
 13. El proveedor local deberá contar como mínimo con 2 técnicos certificados con las certificaciones avanzadas del producto de detección y respuesta extendida XDR.
 14. El proveedor local deberá contar como mínimo con 2 técnicos con certificaciones de cifrado.
 15. El proveedor local deberá contar como mínimo con 2 técnicos con certificaciones en protección de servidores de correo antispam.

16. Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar certificados de inscripción en IPS.
17. 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.
18. 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.
19. El proveedor deberá presentar autorización del fabricante expresamente dirigido a la convocante refiriendo el nro. de ID del llamado.
20. 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.
21. El fabricante de las soluciones ofertadas debe brindar soporte a través de una página web, email y línea telefónica.

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 constituyen los puntos de referencia contra los cuales la convocante podrá verificar el cumplimiento técnico de las ofertas y posteriormente evaluarlas. Por lo tanto, unas EETT bien definidas facilitarán a los oferentes la preparación de ofertas que se ajusten a los documentos de licitación, y a la convocante el examen, evaluación y comparación de las ofertas.
- En las EETT se deberá estipular que todos los bienes o materiales que se incorporen en los bienes deberán ser nuevos, sin uso y del modelo más reciente o actual, y que contendrán todos los perfeccionamientos recientes en materia de diseño y materiales, a menos que en el contrato se disponga otra cosa.
- En las EETT se utilizarán las mejores prácticas. Ejemplos de especificaciones de adquisiciones similares satisfactorias en el mismo sector podrán proporcionar bases concretas para redactar las EETT.
- Las EETT deberán ser lo suficientemente amplias para evitar restricciones relativas a manufactura, materiales, y equipo generalmente utilizados en la fabricación de bienes similares.
- Las normas de calidad del equipo, materiales y manufactura especificadas en los Documentos de Licitación no deberán ser restrictivas. Siempre que sea posible deberán especificarse normas de calidad internacionales. Se deberán evitar referencias a marcas, números de catálogos u otros detalles que limiten los materiales o artículos a un fabricante en particular. Cuando sean inevitables dichas descripciones, siempre deberá estar seguida de expresiones tales como "o sustancialmente equivalente" u "o por lo menos equivalente". 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 avaluos de funcionamiento cubiertas por la garantía, y las especificaciones de las multas aplicables en caso de que dichos avaluos 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 al Formulario de Presentación de la 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 una parte de o todas las Especificaciones Técnicas, cronogramas técnicos, u otra información técnica, la convocante deberá especificar detalladamente la naturaleza y alcance de 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	Descripción del Bien	Especificaciones Técnicas N°
1	ADQUISICIÓN Y ACTUALIZACIÓN DE SOFTWARE DE CIBERSEGURIDAD (KASPERSKY) A SOLUCION DE DETECCION Y RESPUESTA EXTENDIDA (XDR)	EETT N° 19052020-1

De las MIPYMES

Para los procedimientos de Menor Cuantía, este tipo de procedimiento de contratación estará preferentemente reservado a las MIPYMES, de conformidad al artículo 34 inc b) de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas". 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 5° de 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. Así mismo, de los documentos de embarque y otros que deberá suministrar el proveedor indicado a continuación:

Item	Descripción del Bien	Cantidad	Unidad de medida	Lugar de entrega de los Bienes	Fecha(s) final(es) de Entrega de los Bienes
1	ADQUISICIÓN Y ACTUALIZACIÓN DE SOFTWARE DE CIBERSEGURIDAD (KASPERSKY) A SOLUCION DE DETECCION Y RESPUESTA EXTENDIDA (XDR)	4.000	Unidad	Edificio de la ANDE Central (Sito en Avda. España N° 1268 y Padre Cardozo) de Lunes a Viernes de 07:00 a 15:00 hs.	Treinta (30) días calendario. (*)

(*) **Observación:** A partir de la fecha de emisión de la Orden de Entrega a través del Sistema SAP por parte de la Unidad Administradora del Contrato, dentro de los cinco (5) días hábiles de la emisión del código de contratación.

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:

Observar y Respetar el Código de Ética Institucional de la Administración Nacional de Electricidad (ANDE), publicado en www.ande.gov.py.

Las inspecciones y pruebas se realizarán conforme a lo indicado en las Especificaciones Técnicas, si los mismos se ajustan a las características generales y técnicas consignadas en las Especificaciones Técnicas de la Convocante.

Inspecciones de la Contratante:

Una vez que el Proveedor haya cumplido con lo establecido en el Plan de Entregas en el lugar indicado en el mismo, se procederá a una inspección y verificación de los bienes y/o servicios, con los documentos pertinentes.

Documentos de Recepción Provisional y Definitiva:

La Contratante, a través de la Unidad Administradora del Contrato, verificará que los bienes entregados y/o servicios ejecutados, se hayan ajustado a las Especificaciones Técnicas y demás documentos contractuales, para proceder a la emisión del Certificado de Recepción Provisional, a pedido del Proveedor o de oficio, dentro de los treinta (30) días calendario siguientes a la entrega efectuada de conformidad al Plan de Entregas del Contrato o sus eventuales prórrogas autorizadas por la Contratante.

A partir de la fecha de emisión del Certificado de Recepción Provisional correspondiente, se inicia el periodo de garantía indicado en el Pliego de Bases y Condiciones.

Al término de dicho plazo, la Contratante, a través de la Unidad Administradora del Contrato, efectuará las comprobaciones de que el Proveedor ha cumplido satisfactoriamente con todo lo previsto en los documentos del contrato y emitirá dentro de los siguientes treinta (30) días calendario, el Acta de Recepción Definitiva.

Tanto para la Recepción Provisional como para la Recepción Definitiva, en caso de que los bienes entregados y/o servicios ejecutados no se ajusten a las Especificaciones Técnicas y demás documentos contractuales, el Proveedor deberá reparar o reemplazar los bienes y/o subsanar los servicios en el plazo indicado en el Pliego de Bases y Condiciones.

La emisión del Acta de Recepción Definitiva significará el cumplimiento por parte del Proveedor de sus obligaciones contractuales, y le dará derecho a solicitar la cancelación de la Garantía de Cumplimiento del Contrato.

En caso que el Proveedor incurra en atrasos en la entrega de los bienes y/o servicios y le fuere aplicada la multa correspondiente en el Acta de Recepción Definitiva se dejará constancia de ello.

1. El proveedor realizará todas las pruebas y/o inspecciones de los Bienes, por su cuenta y sin costo alguno para la contratante.
2. Las inspecciones y pruebas podrán realizarse en las instalaciones del Proveedor o de sus subcontratistas, en el lugar de entrega y/o en el lugar de destino final de entrega de los bienes, o en otro lugar en este apartado.
- Quando dichas inspecciones o pruebas sean realizadas en recintos del Proveedor o de sus subcontratistas se le proporcionarán a los inspectores todas las facilidades y asistencia razonables, incluso el acceso a los planos y datos sobre producción, sin cargo alguno para la Contratante.
3. La Contratante o su representante designado tendrá derecho a presenciar las pruebas y/o inspecciones mencionadas en la cláusula anterior, siempre y cuando éste asuma todos los costos y gastos que ocasione su participación, incluyendo gastos de viaje, alojamiento y alimentación.
4. Cuando el proveedor esté listo para realizar dichas pruebas e inspecciones, notificará oportunamente a la contratante indicándole el lugar y la hora. El proveedor obtendrá de una tercera parte, si corresponde, o del fabricante cualquier permiso o consentimiento necesario para permitir a la contratante o a su representante designado presenciar las pruebas o inspecciones.
5. La Contratante podrá requerirle al proveedor que realice algunas pruebas y/o inspecciones que no están requeridas en el contrato, pero que considere necesarias para verificar que las características y funcionamiento de los bienes cumplan con los códigos de las especificaciones técnicas y normas establecidas en el contrato. Los costos adicionales razonables que incurra el Proveedor por dichas pruebas e inspecciones serán sumados al precio del contrato, en cuyo caso la contratante deberá justificar a través de un dictamen fundado en el interés público comprometido. Asimismo, si dichas pruebas y/o inspecciones impidieran el avance de la fabricación y/o el desempeño de otras obligaciones del proveedor bajo el Contrato, deberán realizarse los ajustes correspondientes a las Fechas de Entrega y de Cumplimiento y de las otras obligaciones afectadas.
6. El proveedor presentará a la contratante un informe de los resultados de dichas pruebas y/o inspecciones.
7. La contratante podrá rechazar algunos de los bienes o componentes de ellos que no pasen las pruebas o inspecciones o que no se ajusten a las especificaciones. El proveedor tendrá que rectificar o reemplazar dichos bienes o componentes rechazados o hacer las modificaciones necesarias para cumplir con las especificaciones sin ningún costo para la contratante. Asimismo, tendrá que repetir las pruebas o inspecciones, sin ningún costo para la contratante, una vez que notifique a la contratante.

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

Indicadores de Cumplimiento

El documento requerido para acreditar el cumplimiento contractual, será:

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA
Orden de Entrega / Nota de Remisión	Orden de Entrega / Nota de Remisión	Conforme al Plan de Entrega y a las Inspecciones y Pruebas indicados en el Pliego de Bases y Condiciones de la Sección Suministros Requeridos - Especificaciones Técnicas.
Certificado de Recepción Provisional	Certificado de Recepción Provisional	Conforme a las Inspecciones y Pruebas indicados en el Pliego de Bases y Condiciones de la Sección Suministros Requeridos - Especificaciones Técnicas.
Acta de Recepción Definitiva	Acta de Recepción Definitiva	Conforme a las Inspecciones y Pruebas indicados en el Pliego de Bases y Condiciones de la Sección Suministros Requeridos - Especificaciones Técnicas y a las Condiciones Contractuales.

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.

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 calendario, 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.
3. Limitación de Dispensas:
 - a) Toda dispensa a los derechos o facultades de una de las partes en virtud del contrato, deberá ser documentada por escrito, indicar la fecha, estar firmada por un representante autorizado de la parte que otorga dicha dispensa, deberá especificar la obligación dispensada y el alcance de la dispensa.
 - b) Sujeto a lo indicado en el inciso precedente, ningún retraso, prórroga, demora o aprobación por cualquiera de las partes al hacer cumplir algún término y condición del contrato o el otorgar prórrogas por una de las partes a la otra, perjudicará, afectará o limitará los derechos de esa parte en virtud del contrato. Asimismo, ninguna prórroga concedida por cualquiera de las partes por un incumplimiento del contrato, servirá de dispensa para incumplimientos posteriores o continuos del contrato.

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.

1.1. La presentación de los certificados emitidos por las autoridades competentes para cada caso en particular, en el marco de los supuestos del Art. 21 de la Ley N° 7021/22.

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 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 requerir la presentación de los certificados, de conformidad al numeral 1.1, al oferente que resultare adjudicado, con anterioridad a la firma del contrato. Si el oferente no presentare dichos certificados o 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.

Subcontratación

El porcentaje permitido para la subcontratación será de:

No Aplica

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.

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:

La responsabilidad por el transporte de los bienes hasta el lugar de entrega de los bienes recaerá en el Proveedor.

Confidencialidad de la información

1. 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. 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". 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.

2. 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.

3. 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.

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

- a. La contratante o el proveedor requieran compartir con otras instituciones que participan en el financiamiento del contrato,
- b. Actualmente o en el futuro se hace de dominio público sin culpa de ninguna de las partes,
- c. 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
- d. Que de otra manera fue legalmente puesta a la disponibilidad de esa parte por un tercero que no tenía obligación de confidencialidad.

5. 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.

6. 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 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 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 de:

Desde la firma del Contrato hasta la emisión del Acta de Recepción Definitiva.

La cobertura de dicha garantía de cumplimiento de Contrato deberá incluir: Plazo de Entrega; treinta (30) días corridos; Plazo de emisión del Certificado de Recepción Provisional; treinta (30) días corridos; Plazo de Garantía de los Bienes; mil noventa y cinco (1.095) días corridos; Plazo de emisión de Acta de Recepción Definitiva; treinta (30) días corridos más treinta (30) días corridos posteriores al plazo de vigencia del contrato.

Totalizando la cobertura de dicha garantía de cumplimiento de contrato a partir de la vigencia del contrato: Mil doscientos quince (1.215) días corridos.

La Garantía de Cumplimiento de Contrato deberá ser presentada en el Departamento de Seguros - Sede Central de la ANDE - 5to. Piso, dentro del plazo indicado en el apartado porcentaje de Garantía de Fiel Cumplimiento de Contrato y remitir una copia a la Unidad Administradora del Contrato.

En circunstancias motivadas, se solicitará al Proveedor que presente prórrogas de vigencia de las Garantías, las cuales deberán ser presentadas en el Departamento de Seguros de ANDE, en el plazo de veinte (20) días antes del vencimiento de los mismos.

La falta de constitución y/o entrega oportuna de las prórrogas de la Garantía de Fiel Cumplimiento será causal de la ejecución de la misma y rescisión del Contrato por responsabilidad del Proveedor y posteriormente comunicado a la Dirección Nacional de Contrataciones Públicas.

Dentro de los treinta (30) días corridos posteriores a la emisión del Acta de Recepción Definitiva, tendrá lugar la liberación de la Garantía de Cumplimiento de Contrato.

Si la entrega de los bienes o la prestación de los servicios, se realizare en un plazo menor o igual a diez (10) días calendario 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:

- Nota de remisión u orden de prestación de servicios según el objeto de la contratación;
- 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;
- REPSE (registro de prestadores de servicios) todos los que son prestadores de servicios;
- Certificado de Cumplimiento Tributario;
- Constancia de Cumplimiento con la Seguridad Social;
- Formulario de Identificación de Servicios Personales (FIS).

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

a) Los pagos se realizarán en base a los precios que figuran en la Lista de Precios dentro de los sesenta (60) días contados a partir de la presentación de la Solicitud de Pago acompañada de la LIQUIDACIÓN PRO FORMA respectivas, correspondientes a los bienes entregados y verificados de conformidad al Plan de Entrega establecido, descontando el monto de las multas si las hubiere.

Se deberá presentar una Certificación de Cuenta Bancaria emitida por el Banco para proceder a realizar los pagos vía transferencia bancaria.

b) La Solicitud de Pago y la Liquidación Pro-forma deberán estar correctamente elaboradas de acuerdo a los formatos que se incluyen al final en la Sección - Formularios. Asimismo, de verificarse defectos en el contenido de los mencionados documentos, estos serán devueltos para su correcta presentación y el plazo en este lapso quedará suspendido.

c) La Unidad Administradora del Contrato realizará la verificación de la LIQUIDACIÓN PRO-FORMA y en caso de no tener ningún reparo, solicitará al Proveedor la remisión de la Factura Legal con fecha del mes vigente al momento de presentación, con fecha límite hasta el día 20.

d) Se retendrá en concepto de contribución de la implementación, operación, desarrollo, mantenimiento y actualización del Sistema de Información de las Contrataciones Públicas (SICP), el equivalente a cero punto cinco por ciento (0,5%) sobre el importe de cada factura, deducido los impuestos correspondientes, conforme a lo establecido en el Art. 277 de la Ley N° 7228 Que aprueba el Presupuesto General de la Nación Vigente para el Ejercicio Fiscal 2024

f) El Proveedor para tener derecho a todo pago deberá cumplir con lo establecido en la Ley N° 2421/04 y sus reglamentaciones, en lo referente a los comprobantes que expidan por las ventas que efectúen y/o servicios que presten a la Institución.

g) La Solicitud de Pago y la Liquidación Pro-forma deberán ser presentadas a través de una Nota por el portal de Mesa de Entrada de ANDE (www.ande.gov.py), el cual generará un número de Expediente y de ID en el Sistema para seguimiento. La Unidad Administradora del Contrato (UAC) verificará el pedido y autorizará el pago, adjuntando los documentos respaldatorios.

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, y después de que la contratante la haya aceptado. Dicha aceptación o rechazo, deberá darse a más tardar en quince (15) días 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).

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

Anticipo MIPYMES

Se otorgará Anticipo MIPYMES:

No Aplica

Solicitud de Pago de Anticipo

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

No Aplica

Forma de Instrumentación de Garantía de anticipo

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

No Aplica

Reajuste

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

En caso de variación del Índice de Precio del Consumidor (IPC) publicado por el Banco Central del Paraguay (BCP), igual o mayor al quince por ciento (15%) respecto al Índice de Precio del Consumidor (IPC) vigente a la fecha de presentación y apertura de ofertas, el precio del Contrato estará sujeto a ajustes de acuerdo a la siguiente fórmula:

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

Dónde:

Ap = Ajuste de Precios

P = Precio del Contrato

IPC1 = Índice de Precio del Consumidor publicado por el Banco Central del Paraguay correspondiente al mes de entrega del bien.

IPC0 = Índice de Precio del Consumidor publicado por el Banco Central del Paraguay correspondiente al mes de presentación y apertura de ofertas.

El Proveedor presentará las facturas por ajustes en forma independiente de las facturas específicas de las entregas efectuadas.

En caso que el Proveedor se halle atrasado con respecto al Plan de Entrega del Contrato, no se reconocerá el ajuste de precios a favor del mismo.

El ajuste será aplicado a aquella parte del bien pendiente de entrega luego de la variación del Índice de Precio del Consumidor (IPC).

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:

0,10 %

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:

0,001

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 o dentro del plazo establecido en la presente cláusula, 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:

El Proveedor será responsable del pago de todos los impuestos y otros tributos o gravámenes.

Convenios Modificatorios

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

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

Limitación de responsabilidad

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

Responsabilidad del proveedor

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

Fuerza mayor

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

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

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

Causales de terminación del contrato

1. Terminación por Incumplimiento

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

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

2. Terminación por insolvencia o quiebra

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

3. Terminación por conveniencia

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

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

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

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

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

Otras causales de terminación del contrato

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

Por falta de constitución y entrega oportuna de las garantías y eventuales solicitudes de prórroga de las mismas.

Fraude y Corrupción

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

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

- (i) En la etapa de oferta, se descalificará cualquier oferta del oferente y/o rechazará cualquier propuesta de adjudicación relacionada con el proceso de adquisición o contratación de que se trate; y/o
- (ii) Durante la ejecución del contrato, se rescindirá el contrato por causa imputable al proveedor;
- (iii) Se remitirán los antecedentes del oferente o proveedor directamente involucrado en las prácticas fraudulentas o corruptivas, a la Dirección Nacional de Contrataciones Públicas, a los efectos de la aplicación de las sanciones previstas.
- (iv) Se presentará la denuncia ante las instancias correspondientes si el hecho conocido se encontrare tipificado en la legislación penal.

Fraude y corrupción comprenden actos como:

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

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

Medio alternativo de Resolución de Conflictos a través del Avenimiento.

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

Medio Alternativo de Resolución de Conflictos a través de la Mediación

El procedimiento de Mediación se podrá llevar a cabo ante:

No Aplica

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

Medio alternativo de Resolución de Conflictos a través del Arbitraje

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

No Aplica

MODELO DE CONTRATO

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

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

FORMULARIOS

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

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

