

**PLIEGO DE BASES Y CONDICIONES**

---

Convocante:

**Secretaria Nacional de Deportes (SND) / Presidencia de la República  
Secretaria Nacional de Deportes**

Nombre de la Licitación:

**ADQUISICIÓN DE LICENCIAS OFFICE, ANTIVIRUS,  
ANTISPAM PARA LA SND**

(versión 1)

ID de Licitación:

**455757**



Modalidad:

**Menor cuantía nacional**

Publicado el:

**14/10/2024**

*"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:	455757	Nombre de la Licitación:	ADQUISICIÓN DE LICENCIAS OFFICE, ANTIVIRUS, ANTISPAM PARA LA SND
Convocante:	Secretaria Nacional de Deportes (SND) / Presidencia de la República	Categoría:	43000000 - Tecnologías de Informacion, Telecomunicaciones y Radiodifusiones
Unidad de Contratación:	Secretaria Nacional de Deportes	Tipo de Procedimiento:	MCN - Menor cuantía nacional

### Etapas y Plazos

Lugar para Realizar Consultas:	Portal del SICP	Fecha Límite de Consultas:	17/10/2024 09:00
Lugar de Entrega de Ofertas:	Mesa de Entrada de la Secretaria Nacional de Deportes (SND) - Avda. Eusebio Ayala y R.I.6 Boquerón, Asunción.	Fecha de Entrega de Ofertas:	22/10/2024 10:00
Lugar de Apertura de Ofertas:	Oficina Administrativa de la UOC, Avda. Eusebio Ayala y R.I.6 Boquerón, Asunción.	Fecha de Apertura de Ofertas:	22/10/2024 10:30

### Adjudicación y Contrato

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

### Datos del Contacto

Nombre:	Abog. Luis Rolando Portillo	Cargo:	Encargado de la DUOC
Teléfono:	021520673/4	Correo Electrónico:	uoc@snd.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/](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:

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

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:

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

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

4. El precio del contrato que 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 simultaneo, en éste apartado se deberá indicar la manera de distribución de los mismos:

No Aplica

## Moneda de la oferta y pago

La moneda de la oferta y pago será:

Guaranies

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

## Moneda extranjera

En caso de indicar que se permitirá moneda extranjera para la oferta y pago, se debe seleccionar la moneda extranjera permitida:

Guaranies

## 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:

90

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 comprobare que las declaraciones juradas presentadas por el oferente adjudicado con su oferta sean falsas,
  - d.5 No se formaliza el consorcio por escritura pública antes de la firma del contrato.
- 4. En los casos de contratos abiertos las garantías se registrarán por lo dispuesto en el Decreto Reglamentario y la reglamentación emitida por la DNCP para el efecto.
- 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:

120

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:

Si aplica, En cada ítem, el Oferente deberá contar con la Autorización del Fabricante o del Distribuidor Oficial, debidamente acreditado, de la marca en la República del Paraguay.

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:

Los bienes adquiridos deberán funcionar mientras la licencias estén vigentes.

## **Plazo de reposición de bienes**

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

Un (1) día hábil, desde la comunicación 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:

Un (1) año a partir de la recepción.

---

## **Cobertura de Seguro de los bienes**

La cobertura de seguro requerida a los bienes será:

No Aplica

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

# REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN

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

## Condición de Participación

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

Los oferentes domiciliados en la República del Paraguay, que pretendan participar en un procedimiento de contratación, no deberán estar comprendidos en las prohibiciones o limitaciones para presentar propuestas y contratar con el Estado, establecidas en 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.

## Metodo 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:

Los oferentes deberán considerar como **mínimo** la siguiente estructura para cada ítem, en caso de superar los parámetros establecidos para los precios referenciales, al momento de su justificación.

Elementos que determinan el precio del bien	Costo del bien expresado en la moneda de la oferta
Insumos	
Gastos Administrativos	
Total de costos	

Utilidad esperada	
Precio del bien antes de impuestos	
Impuestos	
Precio final del bien impuestos incluidos	

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

## 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:

1. El empleo de los recursos humanos del país.
2. 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.*

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

### 8.1. Personas Físicas.

- a. Fotocopia simple de la Cédula de Identidad del firmante de la oferta. (\*)

b. Constancia de inscripción en el Registro Único de Contribuyentes – RUC (\*)

c. En el caso que suscriba la oferta otra persona en su representación, deberá acompañar una fotocopia simple de su cédula de identidad y una fotocopia simple del poder suficiente otorgado por Escritura Pública para presentar la oferta y representarlo en los actos de la licitación. No es necesario que el poder esté inscripto en el Registro de Poderes. (\*)

#### 8.2. Personas Jurídicas.

1. 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. (\*)
2. Constancia de inscripción en el Registro Único de Contribuyentes. (\*)
3. Fotocopia simple de los documentos de identidad de los representantes o apoderados de la sociedad. (\*)
- d. Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al oferente. Estos documentos pueden consistir en: un poder suficiente 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.

- a. 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. (\*)
- b. 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). (\*)
- c. Fotocopia simple de los documentos que acrediten las facultades de los firmantes del acuerdo de intención de consorciarse. Estos documentos pueden consistir en (\*):
  - i. Un poder suficiente otorgado por escritura pública por cada miembro del consorcio (no es necesario que esté inscripto en el Registro de Poderes); o
  - ii. 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.
- d. 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 (\*):
  - i. 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
  - ii. 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:

Para contribuyente de IRACIS/IRE GENERAL, IRPC/IRE SIMPLE, IRP e IVA GENERAL. AÑOS 2021, 2022, 2023.-

1) Para contribuyentes de IRACIS/IRE GENERAL: Deberá cumplir con el siguiente parámetro de los años (2021, 2022, 2023). -

Deberán cumplir con el siguiente parámetro:

a. **Ratio de Liquidez:** activo corriente / pasivo corriente Deberá ser igual o mayor que 1, en promedio, en los 3 últimos años (2021, 2022, 2023).

b. **Endeudamiento:** pasivo total / activo total No deberá ser mayor a 0,80 en promedio, en los 3 últimos años (2021, 2022, 2023).

c. **Rentabilidad:** Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital. El promedio en los últimos 3 años (2021, 2022, 2023), no deberá ser negativo.

2) Para contribuyentes de IRPC/IRE SIMPLE:

Deberán cumplir el siguiente parámetro: Eficiencia: (Ingreso/Egreso). Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales 2021, 2022, 2023 requeridos.

3) Contribuyente de IRP Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso). Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales 2021, 2022, 2023 requeridos.

4) Contribuyente exclusivamente del IVA General Deberá cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso). Deberá ser igual o mayor que 1, el promedio, de los último 12 meses.

Para los casos de Consorcios, se requerirá que todos los integrantes del mismo cumplan con la totalidad de lo requerido en la Capacidad Financiera.

## Requisitos documentales para la evaluación de la capacidad financiera

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

a	Balance General y Cuadro de Resultados de los años 2.021, 2.022 y 2.023 para contribuyentes de IRACIS/IRE, acorde a las normas contables y a los modelos establecidos en las Normativas Vigentes de la Dirección Nacional de Ingresos Tributarios ( <a href="http://www.dnit.gov.py">www.dnit.gov.py</a> ).
b	Formulario de liquidación de impuesto de IRP o IRPC o su equivalente según la nueva reglamentación tributaria de los años 2.021, 2.022 y 2.023
c	IVA General de los últimos 12 meses, 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 **LICENCIAS** con facturaciones de venta, contratos y/o recepciones finales u otros documentos, por un monto equivalente al 50 % como mínimo del monto total ofertado en el presente procedimiento de contratación, de los últimos 3 (Tres) años (2021, 2022 y 2023) en Instituciones públicas y/o privadas. Las sumatorias de las facturaciones deben alcanzar el porcentaje indicado, no será necesaria la presentación del porcentaje del monto establecido por cada año.

## Requisitos documentales para la evaluación de la experiencia



1. Copia de facturaciones y/o recepciones finales que avalen la experiencia requerida.
2. Copia de contratos con entidades públicas y/o privadas dentro de los años requeridos.
3. *Patente Comercial Vigente del municipio donde esté asentado el establecimiento principal del oferente.*

## Capacidad Técnica

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

1. Declaración Jurada de conocer y aceptar el Pliego de Bases y Condiciones del presente llamado.
2. El proveedor deberá con Recursos Humanos capacitados para realizar la provisión de Software y soporte.
  - \* Deberá contar con al menos 2 técnicos radicados en el país con experiencia en el uso del software para instalación/configuración y capacitación, que formará parte del plantel técnico de instalación/soporte; o mínimo un (1) técnico certificado en Microsoft 365 Certified: Modern Desktop Administrator Associate; o mínimo un (1) técnico certificado en Microsoft Certified Solutions Associate - Office 365.
3. Deberá acreditar la autorización del fabricante y/o Representante, y/o Distribuidor y condiciones de realizar instalación, configuración y soporte del software, según lo solicitado en la planilla de especificaciones técnicas, de acuerdo con lo establecido en las Condiciones Generales.
4. Certificado Internacional en Sistemas de Gestión de Calidad y de la Seguridad de la Información;
  - \* Certificación ISO 9001:2015 gestión de calidad o similar con alcance de integración de software, soporte y o seguridad de la información para instituciones del gobierno;
  - \* Certificación ISO 27001:2013 gestión de la seguridad de la información o similar con alcance de integración de software, soporte y de seguridad de la información para instituciones del gobierno.

## Requisitos documentales para evaluar el criterio de capacidad técnica

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

1. Declaración Jurada de conocer y aceptar el Pliego de Bases y Condiciones del presente llamado.
2. Curriculum Vitae y certificados de los técnicos que en su conjunto cuenten con las siguientes certificaciones ;
  - \* Mínimo un (1) técnico certificado en Microsoft 365 Certified: Modern Desktop Administrator Associate;
  - \* Mínimo un (1) técnico certificado en Microsoft Certified Solutions Associate - Office 365.
3. Carta de Autorización del fabricante y/o Representante y/o distribuidor dirigido a la Institución.
4. Certificados Internacionales;
  - \* Certificación ISO 9001:2015 gestión de calidad o similar, la similitud debe basarse en los mínimos criterios que solicita o Certifica la norma ISO 9001/2015 con respecto a la calidad de la gestión de procedimientos de provisión e integración de bienes y/o servicios.
  - \* Certificación ISO 27001/2013 con respecto a la gestión de la seguridad, confidencialidad e integridad de los datos.

## Otros criterios que la convocante requiera

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

Presentar DECLARACIÓN JURADA DE ESTAR O NO ESTAR INCURSO/A EN CAUSALES DE LOS DEBERES DE ABSTENCIÓN EN CASO DE CONFLICTOS DE INTERESES EN RELACIÓN A FUNCIONARIOS PÚBLICOS, de conformidad con el formulario estándar - sección formularios.

## 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, igualen en precio y sean sus ofertas las más bajas, el comité de evaluación determinará cuál de ellas es la mejor calificada para ejecutar el contrato utilizando los criterios dispuestos para el efecto por la DNCP en la reglamentación pertinente.

## Criterios de Adjudicación

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

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

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

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

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

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

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

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

## 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 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:

- **Identificar el nombre, cargo y la dependencia de la Institución de quien solicita el procedimiento de contratación a ser publicado.** LIC. ROBERTO BOGARIN, JEFE DE DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN.
- **Justificación de la necesidad que se pretende satisfacer mediante la contratación a ser realizada.** La adquisición de soluciones de seguridad informática y productividad como antivirus, Microsoft Office 365 y antivirus antispam por parte de la Secretaría Nacional de Deportes (SND) es una inversión estratégica que busca garantizar la integridad de la información, optimizar los procesos internos y mejorar la eficiencia operativa. A continuación, se presenta una justificación técnica detallada de cada uno de los ítems solicitados.
- **Justificación de la planificación, si se trata de un procedimiento de contratación periódico o sucesivo, o si el mismo responde a una necesidad temporal.** La Secretaría Nacional de Deportes la realiza de manera temporal
- **Justificación de las especificaciones técnicas establecidas.** La adquisición de estos tres productos es fundamental para garantizar la seguridad de la información de la SND, mejorar la productividad de los empleados y cumplir con las normativas vigentes. Al invertir en soluciones de seguridad y productividad, la SND está demostrando su compromiso con la protección de los activos de la institución y con la mejora continua de sus procesos internos.

## Especificaciones técnicas - CPS

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

### ESPECIFICACIONES TÉCNICAS

#### ITEM 1 - Licencia Antivirus

Características	Descripción	Exigencia	Cumple / No Cumple
Marca	Indicar	Exigido	
Modelo	Indicar	Exigido	
Procedencia	Indicar	Exigido	
Cantidad	70 unidades	Exigido	
Suscripción	Mínimo de 1 (un) año	Exigido	
Consola de Administración	La administración deberá ser a través de una consola central única, basada en web y en nube, que deberá contener todas las componentes para el monitoreo y control de la protección de los dispositivos	Exigido	
	La consola deberá presentar un Dashboard con el resumen del estado de protección de los ordenadores y usuarios, así como indicar las alertas de eventos de criticidades alta, media e informativa	Exigido	
	Debe poseer un mecanismo de comunicación vía API, para su integración con otras soluciones de seguridad, como por ejemplo SIEM	Exigido	
	La consola debe permitir la división de los ordenadores dentro de la estructura de administración en grupos	Exigido	
	Debe permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección.	Exigido	
	Debe poseer la posibilidad de aplicar reglas diferenciadas por grupos de usuarios, usuarios individuales, grupos de máquinas y equipos individuales	Exigido	
	La instalación debe poder realizarse a través del cliente descargado de la consola central y también vía correo electrónico de configuración. El instalador debe permitir la distribución del cliente a través de Active Directory (AD) para múltiples máquinas.	Exigido	
	Proporcionar actualizaciones del producto y de las definiciones de virus y protección contra intrusos	Exigido	
	Debe permitir exclusiones de escaneo para un determinado sitio web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política.	Exigido	
	La consola de administración debe permitir la definición de grupos de usuarios con diferentes niveles de acceso a la configuración, las políticas y los registros	Exigido	

Actualización incremental, remota y en tiempo real, de las vacunas de los Antivirus y del mecanismo de verificación (Engine) de los clientes	Exigido	
Permitir la programación de la exploración contra virus con la posibilidad de seleccionar una máquina o grupo de máquinas, con periodicidad definida por el administrador	Exigido	
Utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los clientes administrados.	Exigido	
Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.	Exigido	
Permitir la exportación de los informes gerenciales a los formatos CSV y PDF	Exigido	
Posibilidad de mostrar información como nombre de la máquina, versión del antivirus, sistema operativo, dirección IP, versión del motor, fecha de la actualización, fecha de la última verificación, eventos recientes y estado	Exigido	
La comunicación debe permitir QoS para controlar el ancho de banda de red.	Exigido	
Debe permitir seleccionar un grupo de equipos para aplicar la actualización para controlar el ancho de banda de red. La actualización de la versión debe ser transparente para los usuarios finales.	Exigido	
La herramienta de administración centralizada debe administrar todos los componentes de la protección para estaciones de y debe diseñarse para administrar, supervisar y elaborar informes de endpoint.	Exigido	
La Consola de administración debe incluir un panel con un resumen visual en tiempo real para comprobar el estado de seguridad	Exigido	
Deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los ordenadores que necesitan atención	Exigido	
Deberá mostrar los ordenadores administrados de acuerdo con los criterios de categoría (detalles del estado del equipo, detalles sobre la actualización, detalles de avisos y errores, detalles del antivirus, etc.), y ordenar los equipos en consecuencia	Exigido	
Actualizar de forma automática las directivas de seguridad cuando un equipo se mueve de un grupo a otro	Exigido	
Grabar un registro de auditoría seguro que supervise la actividad en la consola de administración para el cumplimiento de regulaciones, auditorías de seguridad, análisis y solución de problemas forenses	Exigido	
Deberá permitir exportar el informe de registros de auditoría en formatos CSV y PDF	Exigido	

	Debe contener varios informes para el análisis y control de los usuarios y endpoints. Los informes se deben dividir, como mínimo, en informes de: eventos, usuarios, control de aplicaciones, periféricos y web, indicando todas las funciones solicitadas para los endpoints	Exigido	
	Permitir la ejecución manual de todos estos informes, así como la programación y envío automático por correo electrónico en los formatos CSV y PDF	Exigido	
	Debe realizar envío automático de alertas críticas mediante correo electrónico a los administradores	Exigido	
Capacidad de generación de informes	Detalle de usuarios activos, inactivos o desprotegidos, así como detalles de los mismos	Exigido	
	Detalle de los ordenadores que están activos, inactivos o desprotegidos, así como detalles de las exploraciones y alertas en los ordenadores	Exigido	
	Detalle de los periféricos permitidos o bloqueados, así como detalles de dónde y cuándo se utilizó cada periférico	Exigido	
	Detalle de las principales aplicaciones bloqueadas y los servidores / usuarios que intentaron acceder a ellas	Exigido	
	Detalle de las aplicaciones permitidas que fueron accedidas con mayor frecuencia y los servidores / usuarios que las acceden	Exigido	
	Detalle de los servidores / usuarios que intentaron acceder a aplicaciones bloqueadas con mayor frecuencia y las aplicaciones que ellos intentaron acceder	Exigido	
	Detalle de todas las actividades disparadas por reglas de fuga de información.	Exigido	
Opciones de corrección de problemas	Proteger el dispositivo con la opción de inicio de una exploración	Exigido	
	Forzar una actualización en ese momento	Exigido	
	Ver los detalles de los eventos ocurridos	Exigido	
	Ejecutar la comprobación completa del sistema	Exigido	
	Forzar el cumplimiento de una nueva política de seguridad	Exigido	
	Mover el equipo a otro grupo	Exigido	
	Borrar el equipo de la lista	Exigido	



Características básicas del agente de protección	El agente antivirus debe proteger computadoras portátiles, escritorios y servidores en tiempo real, bajo demanda o programado para detectar, bloquear y limpiar todos los virus, troyanos, gusanos y spyware. En Windows, el agente también debe detectar PUA, adware y comportamiento sospechoso	Exigido	
	Además del control de amenazas, el mismo agente (al menos Windows) debe proporcionar control de dispositivos, control de aplicaciones, control web y prevención de fuga de información (DLP).	Exigido	
	Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido	Exigido	
	Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA)	Exigido	
	Debe proteger las funciones críticas en los navegadores de Internet (Safe Browsing)	Exigido	
	Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos	Exigido	
	Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo virus, spyware, troyanos, gusanos, adware y aplicaciones potencialmente no deseadas (PUA)	Exigido	
	Posee la funcionalidad de protección contra el cambio de la configuración del agente, impidiendo a los usuarios, incluyendo el administrador local, reconfigurar, deshabilitar o desinstalar componentes de la solución de protección	Exigido	
	Debe tener un mecanismo contra la desinstalación del endpoint por el usuario y cada dispositivo deberá tener una contraseña única, no siendo autorizadas soluciones con una contraseña que funcione en todos los dispositivos	Exigido	
	Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de los componentes de protección	Exigido	
	Ser capaz de aplicar un análisis adicional, inspeccionando finamente el comportamiento de los códigos durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.	Exigido	
	Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits	Exigido	
	Debe permitir el monitoreo y el control de dispositivos extraíbles en los equipos de los usuarios, como dispositivos USB, periféricos de la propia estación de trabajo y redes inalámbricas, aplicando estas políticas tanto para usuarios como para dispositivo	Exigido	
	El control de dispositivos debe estar al nivel de permiso, sólo lectura o bloqueo	Exigido	

Los siguientes dispositivos deben ser, como mínimo, administrados: HD (hard disks) externos, pendrives USB, almacenables removibles seguras, CD, DVD, Blu-ray, floppy drives, interfaces de red inalámbrica, módems, bluetooth, infrarrojo, MTP (Media Transfer Protocol) y PTP (Picture Transfer Protocol) como cámaras digitales	Exigido	
Control de aplicaciones para monitorear e impedir que los usuarios ejecuten o instalen aplicaciones que puedan afectar la productividad o el rendimiento de la red	Exigido	
Capacidad de reconocer y bloquear automáticamente las aplicaciones en los clientes basándose en la huella digital (hash) del archivo.	Exigido	
Actualización automática de la lista de aplicaciones que se pueden controlar, permitiendo aplicaciones específicas o las categorías específicas de aplicaciones que pueden ser liberadas o bloqueadas	Exigido	
Detectar aplicaciones controladas cuando los usuarios acceden, con las opciones de permitir y alertar o bloquear y alertar	Exigido	
Debe contar con prevención de intrusión en el host (HIPS), que monitoree el código y bloques de código que pueden comportarse de forma maliciosa antes de ser ejecutados	Exigido	
Control de acceso a sitios web por categoría	Exigido	
El Control Web debe controlar el acceso a sitios inapropiados, con al menos 14 categorías de sitios inadecuados. También debe permitir la creación de listas blancas y listas negras.	Exigido	
La aplicación de políticas de control web, debe contar con capacidad de horarios.	Exigido	
Debe poseer protección de fugas o pérdida de datos sensibles en el mismo agente de protección, considerando su contenido, además de la posibilidad de evaluar la extensión del archivo y múltiples destinos	Exigido	
Permitir la identificación de información confidencial, como números de pasaporte u otra información personal identificable y / o información confidencial, incluso si los documentos no se han clasificado correctamente, utilizando CCL (Lista de control de contenido)	Exigido	
Posibilitar el bloqueo, sólo registrar el evento en la Consola de administración, o preguntar al usuario si él o ella realmente quiere transferir el archivo identificado como sensible	Exigido	
Soportar agregar reglas propias de contenido con un asistente proporcionado para este propósito	Exigido	
Capacidad de autorizar, bloquear y confirmar el movimiento de información sensible y en todos los casos, grabar la operación realizada con las principales informaciones de la operación	Exigido	

	El Agente para servidores debe contemplar monitoreo de integridad de archivos, al menos en servidores Windows.	Exigido	
Identificadores de listas CCL preconfiguradas	Números de tarjetas de crédito	Exigido	
	Números de cuentas bancarias	Exigido	
	Números de pasaportes	Exigido	
	Direcciones	Exigido	
	Números de teléfono	Exigido	
	Lista de correos electrónicos	Exigido	
Medios para control de datos	Adjunto en el cliente de correo electrónico (al menos Outlook y Outlook Express)	Exigido	
	Adjunto en el navegador (al menos IE, Firefox y Chrome)	Exigido	
	Adjunto en el cliente de mensajería instantánea (al menos Skype)	Exigido	
	Adjunto a dispositivos de almacenamiento (al menos USB, CD / DVD)	Exigido	
Funcionalidad de detección proactiva de reconocimiento de nuevas amenaza	Protección de amenazas de día 0 a través de tecnología de deep learning (signature less).	Exigido	
	Funcionalidad de detección de amenazas desconocidas que están en memoria	Exigido	
	Capacidad de detección, y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria	Exigido	
	Capacidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria	Exigido	
	No debe requerir descarga de firmas de ningún tipo.	Exigido	
	Capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.	Exigido	
	Análisis forense de lo sucedido, para entender cuál fue la causa raíz del problema con el detalle de los procesos y sub-procesos ejecutados, la lectura y escritura de archivos y de las claves de registro.	Exigido	

	Bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).	Exigido	
	Generación de excepciones ante falsos positivos.	Exigido	
Funcionalidad de protección contra ransomware	Disponer de capacidad de protección contra ransomware basada en comportamiento	Exigido	
	Disponer de capacidad de remediación de la acción de encriptación de los ransomware	Exigido	
	Capacidad de detección del cifrado malicioso de forma local o remoto	Exigido	
	Debe poseer protección anti-ransomware para el sector de booteo (master boot record).	Exigido	
	Debe restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.	Exigido	
	Debe informar a la consola todo el detalle del incidente análisis de causa raíz sin la necesidad de instalar otro agente o dispositivo en la red	Exigido	
Protección contra Vulnerabilidades y técnicas de explotación	Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidades conocidas o de día cero	Exigido	
	Mitigación de inyección de códigos en procesos	Exigido	
	Protección contra robo de credenciales	Exigido	
	Protección contra malware escondido en aplicaciones legítimas (code cave)	Exigido	
	Evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.	Exigido	
	Evitar obtener escalamiento de privilegios	Exigido	
	Modificación de las claves de registro para la ejecución de código arbitrario	Exigido	
Funcionalidades de la protección de correo	Escaneo de mensajes entrantes y salientes	Exigido	
	Políticas de Dominio/Grupo/Usuario	Exigido	
	Cuarentenas de Administradores y Usuarios	Exigido	
	Listas de Bloquear/Permitir del Administrador	Exigido	

	Sincronización con Active Directory	Exigido	
	Bandeja de entrada de emergencia 24/7	Exigido	
	Filtros Anti-Spam	Exigido	
	Para mensajes entrantes:	Exigido	
	- Sender Policy Framework (SPF)		
	- Domain Keys Identified Mail (DKIM)		
	- Domain Message Authentication Reporting & Conformance (DMARC)		
	Filtros basados en detecciones de Virus	Exigido	
Despliegue Agente	Soportar máquinas con arquitectura de 32 bits y 64 bits	Exigido	
	El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Windows 7 en adelante	Exigido	
	El oferente deberá considerar tres licencias adicionales del software para su instalación en servidores de la entidad.	Exigido	
Catálogo	El oferente deberá presentar catálogos, anexos técnicos, manual de equipo y otras documentaciones que contengan toda la información necesaria del bien ofertado, deberán contener los datos de las Especificaciones Técnicas ofertadas.	Exigido	

Ítem 2 Suscripción de Microsoft Office 365			
Descripción	Característica	Mínimo Exigido	Cumple/No cumple
Microsoft Office 365	Microsoft Office 365 Business Standard - (KLQ-00219 ) Office Microsoft 365 Business Std para Mac/Win(Outlook, Word, Excel, PowerPoint y OneNote,Exchange, teams) (además de Access y Publisher solo para PC) Correo de 50 GB 1 TB One Drive.	Exigido	
Cantidad:	55 unidades	Exigido	
Licenciamiento:	Suscripción de 12 meses, la suscripción deberá estar a favor del SND, utilizando la respectiva cuenta de este.	Exigido	

Ítem 3 Licencia de Protección de Correo Electrónico			
Descripción	Característica	Mínimo Exigido	Cumple/No cumple
Solución Antispam	<p>La solución debe proveer una herramienta en la cual en forma centralizada permita gestionar la solución, con mínimo las siguientes características:</p> <ul style="list-style-type: none"> <li>• Gestionar la protección de la solución en grupos creados o en forma individual.</li> <li>• Ver eventos agrupados por categorías de incidentes o amenazas, para permitir enfocar la atención en los compromisos detectados.</li> <li>• Mostrar en forma gráfica el contexto y relacionamiento de los compromisos detectados.</li> <li>• Integración con trazabilidad gráfica en la que pueda tener un contexto del incidente, y permita trazabilidad cruzada entre todos los componentes.</li> <li>• Visibilidad de logs y estadísticas.</li> <li>• Posibilidad de notificación al usuario final cuando un correo entrante (que lo tenga como usuario destino) ha sido retenido por la solución.</li> <li>• Posibilidad de notificación al usuario final cuando un correo saliente (generado por el usuario) ha sido retenido por la solución.</li> <li>• La solución debe tener la capacidad de almacenar datos de los últimos 90 días, y tenerlos disponibles para análisis en base a las características del dashboard integral.</li> <li>• Capacidad de exportación de logs a plataformas externas (SIEM/SOC) en formatos estándares del mercado.</li> <li>• Capacidad de integración por medio de API´s abiertas a consolas externas centralizadas.</li> <li>• Mostrar a nivel de reporte las direcciones de correo electrónico que recibieron la mayor cantidad de mensajes relacionados con Business Email Compromise (BEC).</li> </ul> <ol style="list-style-type: none"> <li>1. Configuración y administración <ol style="list-style-type: none"> <li>a. Debe ser compatible con Microsoft Exchange Online y Microsoft Office 365</li> <li>b. Debe ser compatible con Microsoft Exchange 2003 o posterior.</li> <li>c. En el caso de Microsoft office 365, debe tener la capacidad de integrarse vía API sin la necesidad de modificar registros DNS.</li> <li>d. Debe ser compatible con G Suite de Google Cloud</li> <li>e. Debe ser compatible con cualquier servicio de correo en el que sea propietario del dominio y controle los registros DNS asociados.</li> <li>f. Debe tener la capacidad de sincronizarse con Microsoft Active Directory</li> <li>g. Debe tener la capacidad de sincronizar con Microsoft Azure Active Directory</li> <li>h. Debe tener la capacidad de soportar múltiples dominios para la misma organización.</li> <li>i. Debe poder mantener a los usuarios sincronizados automáticamente con el producto mediante ADSync.</li> <li>j. Debe proporcionar al administrador la capacidad de agregar manualmente registros de alias de direcciones de correo electrónico cuando Active Directory no esté disponible.</li> <li>k. La solución debe tener la capacidad de crear diferentes tipos de roles para la gestión / administración de la plataforma.</li> <li>l. Debe proporcionar al administrador la capacidad de encontrar buzones de correo específicos.</li> <li>m. Debe tener un portal de autoservicio para usuarios finales.</li> </ol> </li> </ol>	Exigido	

- n. El portal de autoservicio debe permitir a los usuarios administrar correos electrónicos en cuarentena (aceptar / eliminar correos electrónicos)
  - o. El portal de autoservicio debe permitir a los usuarios editar las reglas de permitir / bloquear
  - p. El portal de autoservicio debe permitir a los usuarios ver los mensajes en caso de interrupción utilizando la bandeja de entrada de emergencia.
  - q. Debe proporcionar a los usuarios la capacidad de agregar Smart Banners (un sistema de clasificación de colores simple) a cualquier correo electrónico recibido desde fuera de la organización, lo que ayuda a los destinatarios a identificar el riesgo de cada correo electrónico y les permite agregar remitentes a sus listas de permisos y bloqueos con un solo clic.
  - r. Debe poder crear políticas de seguridad de correo electrónico únicas para individuos, grupos o todo el dominio.
  - s. Debe cumplir con las regulaciones de cumplimiento de datos.
  - t. Debe tener una opción de centros de datos globales al momento de la creación de la cuenta, como Reino Unido, EE. UU. Y Alemania
2. Continuidad del negocio
- a. Debe tener la capacidad de manejar una cola de correo electrónico que garantice que no se pierda ningún correo.
  - b. En caso de una interrupción de su servicio de correo electrónico de Microsoft o Google Cloud, el producto debe tener la capacidad de poner en cola automáticamente los correos electrónicos del destinatario y luego entregarlos una vez que se restablezca el servicio con un período de reintento de cinco días.
  - c. Debe proporcionar al usuario acceso a una bandeja de entrada de emergencia 24 horas al día, 7 días a la semana.
  - d. Debe tener la capacidad de enviar alertas cuando el correo no se pueda entregar a un servidor / servicio en caso de interrupciones de un proveedor de servicios de correo electrónico en la nube de terceros.
3. Seguridad
- a. Debe tener actualizaciones de amenazas en vivo para detener los últimos ataques.
  - b. Debe tener detección antispam, antivirus y antiphishing.
  - c. Debe tener un filtro de reputación que pueda bloquear al menos con un 90% del spam.
  - d. Debe tener tecnología de filtrado de reputación de próxima generación que elimine el spam de botnet en el nivel de conexión IP al monitorear las solicitudes de conexión y rechace aquellas que muestren evidencia de conexiones de botnet.
  - e. Debe proteger contra el spam tipo Snowshoe Spamming
  - f. Debe tener un portal para el usuario final que luego permita a los usuarios publicar correos electrónicos bajo demanda y resúmenes de cuarentena en el mensaje que brinden un resumen diario del correo en cuarentena, con la opción de liberarlos directamente desde la bandeja de entrada.
  - g. Debe tener técnicas de autenticación SPF, DKIM y DMARC para identificar y permitir correos electrónicos legítimos mientras bloquea a los impostores.
  - h. Debe tener detección de anomalías en el encabezado que identifique si el nombre para mostrar del remitente es el mismo que un nombre de usuario interno.
4. Protección contra la suplantación de identidad
- a. Debe poder comparar el nombre para mostrar de los correos electrónicos entrantes con el nombre para mostrar de las marcas de servicios en la nube y tener la opción de poder parametrizar usuarios con categoría VIP para evitar la suplantación de identidad dentro de la organización.
  - b. Debe poder hacer un análisis de dominios similares para identificar nombres de dominio de uso corporativo.
  - c. Los mensajes sospechosos se pueden bloquear, poner en cuarentena, etiquetar con una advertencia en la línea de asunto o agregar un banner con un enlace directo a la lista de bloqueo a nivel de usuario.
5. Protección de la información.
- a. Debe escanear automáticamente los cuerpos de los mensajes y los archivos

	<p>adjuntos en busca de datos confidenciales para establecer fácilmente políticas para bloquear o cifrar los mensajes.</p> <p>b. Debe brindar a los usuarios la capacidad de cifrar correos electrónicos utilizando el complemento O365 del producto.</p> <p>c. Debe tener un cifrado basado en inserción que proteja todo el correo electrónico o solo los archivos adjuntos.</p> <p>d. Debe tener un cifrado TLS reforzado que evite las escuchas cuando los mensajes están en tránsito.</p> <p>e. Debe tener capacidades de control de contenido y prevención de pérdida de datos.</p> <p>6. Protección activa contra amenazas</p> <p>a. Debe tener capacidad de reescritura de URL para verificar la reputación del sitio web de los enlaces de correo electrónico antes de la entrega y en el momento en que hace clic, bloqueando ataques furtivos y retardados.</p> <p>b. Debe tener una zona de pruebas basada en la nube que pueda detectar malware conocido y desconocido y aplicaciones no deseadas antes de que se ejecute.</p> <p>7. Informes completos</p> <p>a. Debe contar con un Panel de Control (Dashboard), en donde se ilustre de manera general el comportamiento del estado de los correos electrónicos analizados, así mismo deberá ilustrar que buzones de correo electrónico se encuentran en riesgo.</p> <p>b. Debe proporcionar informes de estadísticas dentro de la consola en forma de tablas y gráficos con rangos de fechas personalizados.</p> <p>c. Debe incluir un informe que proporcione información completa sobre el encabezado del mensaje y cualquier archivo adjunto.</p> <p>d. Debe incluir un informe que proporcione detalles de los pasos por los que pasó el mensaje en la infraestructura de análisis de correo electrónico.</p> <p>e. Debe incluir un reporte sobre detecciones asociadas a la política para prevención de Fuga de Información.</p> <p>f. Debe incluir un Informe de amenazas avanzado que proporcione un resumen de los mensajes entrantes que se detonaron en el entorno de la zona de pruebas, que se puede filtrar por fecha y el resultado del análisis durante el último año.</p>		
Cantidad:	70 unidades	Exigido	
Licenciamiento:	Suscripción de 12 meses, la suscripción deberá estar a favor del SND, utilizando la respectiva cuenta de este.	Exigido	

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:

ESPECIFICACIONES TÉCNICAS			
ITEM 1 - Licencia Antivirus			
Características	Descripción	Exigencia	Cumple / No Cumple
Marca	Indicar	Exigido	
Modelo	Indicar	Exigido	
Procedencia	Indicar	Exigido	
Cantidad	70 unidades	Exigido	
Suscripción	Mínimo de 1 (un) año	Exigido	

Consola de Administración	La administración deberá ser a través de una consola central única, basada en web y en nube, que deberá contener todas las componentes para el monitoreo y control de la protección de los dispositivos	Exigido	
	La consola deberá presentar un Dashboard con el resumen del estado de protección de los ordenadores y usuarios, así como indicar las alertas de eventos de criticidades alta, media e informativa	Exigido	
	Debe poseer un mecanismo de comunicación vía API, para su integración con otras soluciones de seguridad, como por ejemplo SIEM	Exigido	
	La consola debe permitir la división de los ordenadores dentro de la estructura de administración en grupos	Exigido	
	Debe permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección.	Exigido	
	Debe poseer la posibilidad de aplicar reglas diferenciadas por grupos de usuarios, usuarios individuales, grupos de máquinas y equipos individuales	Exigido	
	La instalación debe poder realizarse a través del cliente descargado de la consola central y también vía correo electrónico de configuración. El instalador debe permitir la distribución del cliente a través de Active Directory (AD) para múltiples máquinas.	Exigido	
	Proporcionar actualizaciones del producto y de las definiciones de virus y protección contra intrusos	Exigido	
	Debe permitir exclusiones de escaneo para un determinado sitio web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política.	Exigido	
	La consola de administración debe permitir la definición de grupos de usuarios con diferentes niveles de acceso a la configuración, las políticas y los registros	Exigido	
	Actualización incremental, remota y en tiempo real, de las vacunas de los Antivirus y del mecanismo de verificación (Engine) de los clientes	Exigido	
	Permitir la programación de la exploración contra virus con la posibilidad de seleccionar una máquina o grupo de máquinas, con periodicidad definida por el administrador	Exigido	
	Utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los clientes administrados.	Exigido	
	Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.	Exigido	
	Permitir la exportación de los informes gerenciales a los formatos CSV y PDF	Exigido	

	Posibilidad de mostrar información como nombre de la máquina, versión del antivirus, sistema operativo, dirección IP, versión del motor, fecha de la actualización, fecha de la última verificación, eventos recientes y estado	Exigido	
	La comunicación debe permitir QoS para controlar el ancho de banda de red.	Exigido	
	Debe permitir seleccionar un grupo de equipos para aplicar la actualización para controlar el ancho de banda de red. La actualización de la versión debe ser transparente para los usuarios finales.	Exigido	
	La herramienta de administración centralizada debe administrar todos los componentes de la protección para estaciones de y debe diseñarse para administrar, supervisar y elaborar informes de endpoint.	Exigido	
	La Consola de administración debe incluir un panel con un resumen visual en tiempo real para comprobar el estado de seguridad	Exigido	
	Deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los ordenadores que necesitan atención	Exigido	
	Deberá mostrar los ordenadores administrados de acuerdo con los criterios de categoría (detalles del estado del equipo, detalles sobre la actualización, detalles de avisos y errores, detalles del antivirus, etc.), y ordenar los equipos en consecuencia	Exigido	
	Actualizar de forma automática las directivas de seguridad cuando un equipo se mueve de un grupo a otro	Exigido	
	Grabar un registro de auditoría seguro que supervise la actividad en la consola de administración para el cumplimiento de regulaciones, auditorías de seguridad, análisis y solución de problemas forenses	Exigido	
	Deberá permitir exportar el informe de registros de auditoría en formatos CSV y PDF	Exigido	
	Debe contener varios informes para el análisis y control de los usuarios y endpoints. Los informes se deben dividir, como mínimo, en informes de: eventos, usuarios, control de aplicaciones, periféricos y web, indicando todas las funciones solicitadas para los endpoints	Exigido	
	Permitir la ejecución manual de todos estos informes, así como la programación y envío automático por correo electrónico en los formatos CSV y PDF	Exigido	
	Debe realizar envío automático de alertas críticas mediante correo electrónico a los administradores	Exigido	
Capacidad de generación de informes	Detalle de usuarios activos, inactivos o desprotegidos, así como detalles de los mismos	Exigido	
	Detalle de los ordenadores que están activos, inactivos o desprotegidos, así como detalles de las exploraciones y alertas en los ordenadores	Exigido	

	Detalle de los periféricos permitidos o bloqueados, así como detalles de dónde y cuándo se utilizó cada periférico	Exigido	
	Detalle de las principales aplicaciones bloqueadas y los servidores / usuarios que intentaron acceder a ellas	Exigido	
	Detalle de las aplicaciones permitidas que fueron accedidas con mayor frecuencia y los servidores / usuarios que las acceden	Exigido	
	Detalle de los servidores / usuarios que intentaron acceder a aplicaciones bloqueadas con mayor frecuencia y las aplicaciones que ellos intentaron acceder	Exigido	
	Detalle de todas las actividades disparadas por reglas de fuga de información.	Exigido	
Opciones de corrección de problemas	Proteger el dispositivo con la opción de inicio de una exploración	Exigido	
	Forzar una actualización en ese momento	Exigido	
	Ver los detalles de los eventos ocurridos	Exigido	
	Ejecutar la comprobación completa del sistema	Exigido	
	Forzar el cumplimiento de una nueva política de seguridad	Exigido	
	Mover el equipo a otro grupo	Exigido	
	Borrar el equipo de la lista	Exigido	
Características básicas del agente de protección	El agente antivirus debe proteger computadoras portátiles, escritorios y servidores en tiempo real, bajo demanda o programado para detectar, bloquear y limpiar todos los virus, troyanos, gusanos y spyware. En Windows, el agente también debe detectar PUA, adware y comportamiento sospechoso	Exigido	
	Además del control de amenazas, el mismo agente (al menos Windows) debe proporcionar control de dispositivos, control de aplicaciones, control web y prevención de fuga de información (DLP).	Exigido	
	Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido	Exigido	
	Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA)	Exigido	
	Debe proteger las funciones críticas en los navegadores de Internet (Safe Browsing)	Exigido	
	Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos	Exigido	

Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo virus, spyware, troyanos, gusanos, adware y aplicaciones potencialmente no deseadas (PUA)	Exigido	
Posee la funcionalidad de protección contra el cambio de la configuración del agente, impidiendo a los usuarios, incluyendo el administrador local, reconfigurar, deshabilitar o desinstalar componentes de la solución de protección	Exigido	
Debe tener un mecanismo contra la desinstalación del endpoint por el usuario y cada dispositivo deberá tener una contraseña única, no siendo autorizadas soluciones con una contraseña que funcione en todos los dispositivos	Exigido	
Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de los componentes de protección	Exigido	
Ser capaz de aplicar un análisis adicional, inspeccionando finamente el comportamiento de los códigos durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.	Exigido	
Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits	Exigido	
Debe permitir el monitoreo y el control de dispositivos extraíbles en los equipos de los usuarios, como dispositivos USB, periféricos de la propia estación de trabajo y redes inalámbricas, aplicando estas políticas tanto para usuarios como para dispositivo	Exigido	
El control de dispositivos debe estar al nivel de permiso, sólo lectura o bloqueo	Exigido	
Los siguientes dispositivos deben ser, como mínimo, administrados: HD (hard disks) externos, pendrives USB, almacenables removibles seguras, CD, DVD, Blu-ray, floppy drives, interfaces de red inalámbrica, módems, bluetooth, infrarrojo, MTP (Media Transfer Protocol) y PTP (Picture Transfer Protocol) como cámaras digitales	Exigido	
Control de aplicaciones para monitorear e impedir que los usuarios ejecuten o instalen aplicaciones que puedan afectar la productividad o el rendimiento de la red	Exigido	
Capacidad de reconocer y bloquear automáticamente las aplicaciones en los clientes basándose en la huella digital (hash) del archivo.	Exigido	
Actualización automática de la lista de aplicaciones que se pueden controlar, permitiendo aplicaciones específicas o las categorías específicas de aplicaciones que pueden ser liberadas o bloqueadas	Exigido	
Detectar aplicaciones controladas cuando los usuarios acceden, con las opciones de permitir y alertar o bloquear y alertar	Exigido	
Debe contar con prevención de intrusión en el host (HIPS), que monitoree el código y bloques de código que pueden comportarse de forma maliciosa antes de ser ejecutados	Exigido	

	Control de acceso a sitios web por categoría	Exigido	
	El Control Web debe controlar el acceso a sitios inapropiados, con al menos 14 categorías de sitios inadecuados. También debe permitir la creación de listas blancas y listas negras.	Exigido	
	La aplicación de políticas de control web, debe contar con capacidad de horarios.	Exigido	
	Debe poseer protección de fugas o pérdida de datos sensibles en el mismo agente de protección, considerando su contenido, además de la posibilidad de evaluar la extensión del archivo y múltiples destinos	Exigido	
	Permitir la identificación de información confidencial, como números de pasaporte u otra información personal identificable y / o información confidencial, incluso si los documentos no se han clasificado correctamente, utilizando CCL (Lista de control de contenido)	Exigido	
	Posibilitar el bloqueo, sólo registrar el evento en la Consola de administración, o preguntar al usuario si él o ella realmente quiere transferir el archivo identificado como sensible	Exigido	
	Soportar agregar reglas propias de contenido con un asistente proporcionado para este propósito	Exigido	
	Capacidad de autorizar, bloquear y confirmar el movimiento de información sensible y en todos los casos, grabar la operación realizada con las principales informaciones de la operación	Exigido	
	El Agente para servidores debe contemplar monitoreo de integridad de archivos, al menos en servidores Windows.	Exigido	
Identificadores de listas CCL preconfiguradas	Números de tarjetas de crédito	Exigido	
	Números de cuentas bancarias	Exigido	
	Números de pasaportes	Exigido	
	Direcciones	Exigido	
	Números de teléfono	Exigido	
	Lista de correos electrónicos	Exigido	
Medios para control de datos	Adjunto en el cliente de correo electrónico (al menos Outlook y Outlook Express)	Exigido	
	Adjunto en el navegador (al menos IE, Firefox y Chrome)	Exigido	

	Adjunto en el cliente de mensajería instantánea (al menos Skype)	Exigido	
	Adjunto a dispositivos de almacenamiento (al menos USB, CD / DVD)	Exigido	
Funcionalidad de detección proactiva de reconocimiento de nuevas amenazas	Protección de amenazas de día 0 a través de tecnología de deep learning (signature less).	Exigido	
	Funcionalidad de detección de amenazas desconocidas que están en memoria	Exigido	
	Capacidad de detección, y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria	Exigido	
	Capacidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria	Exigido	
	No debe requerir descarga de firmas de ningún tipo.	Exigido	
	Capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.	Exigido	
	Análisis forense de lo sucedido, para entender cuál fue la causa raíz del problema con el detalle de los procesos y sub-procesos ejecutados, la lectura y escritura de archivos y de las claves de registro.	Exigido	
	Bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).	Exigido	
	Generación de excepciones ante falsos positivos.	Exigido	
Funcionalidad de protección contra ransomware	Disponer de capacidad de protección contra ransomware basada en comportamiento	Exigido	
	Disponer de capacidad de remediación de la acción de encriptación de los ransomware	Exigido	
	Capacidad de detección del cifrado malicioso de forma local o remoto	Exigido	
	Debe poseer protección anti-ransomware para el sector de booteo (master boot record).	Exigido	
	Debe restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.	Exigido	
	Debe informar a la consola todo el detalle del incidente análisis de causa raíz sin la necesidad de instalar otro agente o dispositivo en la red	Exigido	

Protección contra Vulnerabilidades y técnicas de explotación	Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidades conocidas o de día cero	Exigido	
	Mitigación de inyección de códigos en procesos	Exigido	
	Protección contra robo de credenciales	Exigido	
	Protección contra malware escondido en aplicaciones legítimas (code cave)	Exigido	
	Evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.	Exigido	
	Evitar obtener escalamiento de privilegios	Exigido	
	Modificación de las claves de registro para la ejecución de código arbitrario	Exigido	
Funcionalidades de la protección de correo	Escaneo de mensajes entrantes y salientes	Exigido	
	Políticas de Dominio/Grupo/Usuario	Exigido	
	Cuarentenas de Administradores y Usuarios	Exigido	
	Listas de Bloquear/Permitir del Administrador	Exigido	
	Sincronización con Active Directory	Exigido	
	Bandeja de entrada de emergencia 24/7	Exigido	
	Filtros Anti-Spam	Exigido	
	Para mensajes entrantes:	Exigido	
	- Sender Policy Framework (SPF)		
	- Domain Keys Identified Mail (DKIM)		
	- Domain Message Authentication Reporting & Conformance (DMARC)		
	Filtros basados en detecciones de Virus	Exigido	
Despliegue Agente	Soportar máquinas con arquitectura de 32 bits y 64 bits	Exigido	



	El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Windows 7 en adelante	Exigido	
	El oferente deberá considerar tres licencias adicionales del software para su instalación en servidores de la entidad.	Exigido	
Catálogo	El oferente deberá presentar catálogos, anexos técnicos, manual de equipo y otras documentaciones que contengan toda la información necesaria del bien ofertado, deberán contener los datos de las Especificaciones Técnicas ofertadas.	Exigido	

· Ítem 2 Suscripción de Microsoft Office 365			
Descripción	Característica	Mínimo Exigido	Cumple/No cumple
Microsoft Office 365	Microsoft Office 365 Business Standard - (KLQ-00219 ) Office Microsoft 365 Business Std para Mac/Win(Outlook, Word, Excel, PowerPoint y OneNote,Exchange, teams) (además de Access y Publisher solo para PC) Correo de 50 GB 1 TB One Drive.	Exigido	
Cantidad:	55 unidades	Exigido	
Licenciamiento:	Suscripción de 12 meses, la suscripción deberá estar a favor del SND, utilizando la respectiva cuenta de este.	Exigido	

· Ítem 3 Licencia de Protección de Correo Electrónico			
Descripción	Característica	Mínimo Exigido	Cumple/No cumple
Solución Antispam	<p>La solución debe proveer una herramienta en la cual en forma centralizada permita gestionar la solución, con mínimo las siguientes características:</p> <ul style="list-style-type: none"> <li>• Gestionar la protección de la solución en grupos creados o en forma individual.</li> <li>• Ver eventos agrupados por categorías de incidentes o amenazas, para permitir enfocar la atención en los compromisos detectados.</li> <li>• Mostrar en forma gráfica el contexto y relacionamiento de los compromisos detectados.</li> <li>• Integración con trazabilidad gráfica en la que pueda tener un contexto del incidente, y permita trazabilidad cruzada entre todos los componentes.</li> <li>• Visibilidad de logs y estadísticas.</li> <li>• Posibilidad de notificación al usuario final cuando un correo entrante (que lo tenga como usuario destino) ha sido retenido por la solución.</li> <li>• Posibilidad de notificación al usuario final cuando un correo saliente (generado</li> </ul>	Exigido	

por el usuario) ha sido retenido por la solución.

- La solución debe tener la capacidad de almacenar datos de los últimos 90 días, y tenerlos disponibles para análisis en base a las características del dashboard integral.
- Capacidad de exportación de logs a plataformas externas (SIEM/SOC) en formatos estándares del mercado.
- Capacidad de integración por medio de API´s abiertas a consolas externas centralizadas.
- Mostrar a nivel de reporte las direcciones de correo electrónico que recibieron la mayor cantidad de mensajes relacionados con Business Email Compromise (BEC).

1. Configuración y administración

- a. Debe ser compatible con Microsoft Exchange Online y Microsoft Office 365
  - b. Debe ser compatible con Microsoft Exchange 2003 o posterior.
  - c. En el caso de Microsoft office 365, debe tener la capacidad de integrarse vía API sin la necesidad de modificar registros DNS.
  - d. Debe ser compatible con G Suite de Google Cloud
  - e. Debe ser compatible con cualquier servicio de correo en el que sea propietario del dominio y controle los registros DNS asociados.
  - f. Debe tener la capacidad de sincronizarse con Microsoft Active Directory
  - g. Debe tener la capacidad de sincronizar con Microsoft Azure Active Directory
  - h. Debe tener la capacidad de soportar múltiples dominios para la misma organización.
  - i. Debe poder mantener a los usuarios sincronizados automáticamente con el producto mediante ADSync.
  - j. Debe proporcionar al administrador la capacidad de agregar manualmente registros de alias de direcciones de correo electrónico cuando Active Directory no esté disponible.
  - k. La solución debe tener la capacidad de crear diferentes tipos de roles para la gestión / administración de la plataforma.
  - l. Debe proporcionar al administrador la capacidad de encontrar buzones de correo específicos.
  - m. Debe tener un portal de autoservicio para usuarios finales.
  - n. El portal de autoservicio debe permitir a los usuarios administrar correos electrónicos en cuarentena (aceptar / eliminar correos electrónicos)
  - o. El portal de autoservicio debe permitir a los usuarios editar las reglas de permitir / bloquear
  - p. El portal de autoservicio debe permitir a los usuarios ver los mensajes en caso de interrupción utilizando la bandeja de entrada de emergencia.
  - q. Debe proporcionar a los usuarios la capacidad de agregar Smart Banners (un sistema de clasificación de colores simple) a cualquier correo electrónico recibido desde fuera de la organización, lo que ayuda a los destinatarios a identificar el riesgo de cada correo electrónico y les permite agregar remitentes a sus listas de permisos y bloqueos con un solo clic.
  - r. Debe poder crear políticas de seguridad de correo electrónico únicas para individuos, grupos o todo el dominio.
  - s. Debe cumplir con las regulaciones de cumplimiento de datos.
  - t. Debe tener una opción de centros de datos globales al momento de la creación de la cuenta, como Reino Unido, EE. UU. Y Alemania
2. Continuidad del negocio
- a. Debe tener la capacidad de manejar una cola de correo electrónico que garantice que no se pierda ningún correo.
  - b. En caso de una interrupción de su servicio de correo electrónico de Microsoft o Google Cloud, el producto debe tener la capacidad de poner en cola automáticamente los correos electrónicos del destinatario y luego entregarlos una vez que se restablezca el servicio con un período de reintento de cinco días.
  - c. Debe proporcionar al usuario acceso a una bandeja de entrada de emergencia 24

horas al día, 7 días a la semana.

d. Debe tener la capacidad de enviar alertas cuando el correo no se pueda entregar a un servidor / servicio en caso de interrupciones de un proveedor de servicios de correo electrónico en la nube de terceros.

### 3. Seguridad

a. Debe tener actualizaciones de amenazas en vivo para detener los últimos ataques.

b. Debe tener detección antispam, antivirus y antiphishing.

c. Debe tener un filtro de reputación que pueda bloquear al menos con un 90% del spam.

d. Debe tener tecnología de filtrado de reputación de próxima generación que elimine el spam de botnet en el nivel de conexión IP al monitorear las solicitudes de conexión y rechace aquellas que muestren evidencia de conexiones de botnet.

e. Debe proteger contra el spam tipo Snowshoe Spamming

f. Debe tener un portal para el usuario final que luego permita a los usuarios publicar correos electrónicos bajo demanda y resúmenes de cuarentena en el mensaje que brinden un resumen diario del correo en cuarentena, con la opción de liberarlos directamente desde la bandeja de entrada.

g. Debe tener técnicas de autenticación SPF, DKIM y DMARC para identificar y permitir correos electrónicos legítimos mientras bloquea a los impostores.

h. Debe tener detección de anomalías en el encabezado que identifique si el nombre para mostrar del remitente es el mismo que un nombre de usuario interno.

### 4. Protección contra la suplantación de identidad

a. Debe poder comparar el nombre para mostrar de los correos electrónicos entrantes con el nombre para mostrar de las marcas de servicios en la nube y tener la opción de poder parametrizar usuarios con categoría VIP para evitar la suplantación de identidad dentro de la organización.

b. Debe poder hacer un análisis de dominios similares para identificar nombres de dominio de uso corporativo.

c. Los mensajes sospechosos se pueden bloquear, poner en cuarentena, etiquetar con una advertencia en la línea de asunto o agregar un banner con un enlace directo a la lista de bloqueo a nivel de usuario.

### 5. Protección de la información.

a. Debe escanear automáticamente los cuerpos de los mensajes y los archivos adjuntos en busca de datos confidenciales para establecer fácilmente políticas para bloquear o cifrar los mensajes.

b. Debe brindar a los usuarios la capacidad de cifrar correos electrónicos utilizando el complemento O365 del producto.

c. Debe tener un cifrado basado en inserción que proteja todo el correo electrónico o solo los archivos adjuntos.

d. Debe tener un cifrado TLS reforzado que evite las escuchas cuando los mensajes están en tránsito.

e. Debe tener capacidades de control de contenido y prevención de pérdida de datos.

### 6. Protección activa contra amenazas

a. Debe tener capacidad de reescritura de URL para verificar la reputación del sitio web de los enlaces de correo electrónico antes de la entrega y en el momento en que hace clic, bloqueando ataques furtivos y retardados.

b. Debe tener una zona de pruebas basada en la nube que pueda detectar malware conocido y desconocido y aplicaciones no deseadas antes de que se ejecute.

### 7. Informes completos

a. Debe contar con un Panel de Control (Dashboard), en donde se ilustre de manera general el comportamiento del estado de los correos electrónicos analizados, así mismo deberá ilustrar que buzones de correo electrónico se encuentran en riesgo.

b. Debe proporcionar informes de estadísticas dentro de la consola en forma de tablas y gráficos con rangos de fechas personalizados.

c. Debe incluir un informe que proporcione información completa sobre el

	<p>encabezado del mensaje y cualquier archivo adjunto.</p> <p>d. Debe incluir un informe que proporcione detalles de los pasos por los que pasó el mensaje en la infraestructura de análisis de correo electrónico.</p> <p>e. Debe incluir un reporte sobre detecciones asociadas a la política para prevención de Fuga de Información.</p> <p>f. Debe incluir un Informe de amenazas avanzado que proporcione un resumen de los mensajes entrantes que se detonaron en el entorno de la zona de pruebas, que se puede filtrar por fecha y el resultado del análisis durante el último año.</p>		
Cantidad:	70 unidades	Exigido	
Licenciamiento:	Suscripción de 12 meses, la suscripción deberá estar a favor del SND, utilizando la respectiva cuenta de este.	Exigido	

## 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:

La entrega de los bienes se realizará de acuerdo con el plan de entrega, indicado en el presente apartado:

Ítem	Descripción de los Bienes	Cantidad	Lugar de entrega de los Bienes	Fecha(s) final(es) e entrega de los Servicios
1	Licencia de Antivirus	70	Oficina del SND - Sede Av. Eusebio Ayala y R.I. 6 Boquerón	El Plazo es de 3 días posterior a la recepción de la Orden de Compra por parte del proveedor, previa firma del Contrato.
2	Suscripción de Microsoft Office 365	55	Oficina del SND - Sede Av. Eusebio Ayala y R.I. 6 Boquerón	El Plazo es de 3 días posterior a la recepción de la Orden de Compra por parte del proveedor, previa firma del Contrato.

3	Licencia de Protección de Correo Electrónico	70	Oficina del SND - Sede Av. Eusebio Ayala y R.I. 6 Boquerón	El Plazo es de 3 días posterior a la recepción de la Orden de Compra por parte del proveedor, previa firma del Contrato.
---	--	----	--	--

## Planos y diseños

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

No Aplica

## Embalajes y documentos

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

No Aplica

## Inspecciones y pruebas

Las inspecciones y pruebas serán como se indica a continuación:

No Aplica

## Indicadores de Cumplimiento

El documento requerido para acreditar el cumplimiento contractual, será:

INDICADOR

TIPO

FECHA DE PRESENTACIÓN PREVISTA (Se indica la fecha que debe presentar según el PBC)

Orden de entrega / Nota  
de Remisión / Acta de  
recepción

Orden de entrega / Nota  
de Remisión / Acta de  
recepción

Según Orden de entrega emitida.

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:

No Aplica

## 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 fecha de la firma del contrato hasta después de 30 días corridos posteriores al plazo de ejecución o vigencia del contrato, según sea el caso.

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:

1. Nota de remisión u orden de prestación de servicios según el objeto de la contratación;
2. 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;
3. REPSE (registro de prestadores de servicios) todos los que son prestadores de servicios;
4. Certificado de Cumplimiento Tributario;
5. Constancia de Cumplimiento con la Seguridad Social;
6. Formulario de Identificación de Servicios Personales (FIS).

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

- \* Nota dirigida a la Convocante, solicitando el pago
- \* Orden de Compra
- \* Acta de Conformidad emitida por el ADMINISTRADOR DEL CONTRATO

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:

Los precios del contrato estarán sujetos a reajustes, siempre y cuando exista una variación sustancial de precios en la economía nacional y ésta se vea reflejada en el índice de precios de consumo establecido por el Banco Central del Paraguay, en un valor igual o mayor al quince por ciento sobre la inflación oficial esperada para el mismo periodo, conforme a la siguiente fórmula:

$$Pr = P \times \frac{IPC1}{IPC0}$$

Dónde:

Pr: Precio Reajustado.

P: Precio adjudicado

IPC1: Índice de precios al consumidor estimado por el Banco Central del Paraguay para la fecha en que se produce el pedido de reajuste.

IPC0: Índice de precios al consumidor informado por el Banco Central del Paraguay, correspondiente a la fecha en que se solicita el pedido de reajuste.

**No se reconocerán reajustes de precios si el suministro se encuentra atrasado respecto al cronograma de entregas aprobado**

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:

0,01

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:

No Aplica

---

## Convenios Modificatorios

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

1. Cuando el sistema de adjudicación adoptado sea de abastecimiento simultáneo las ampliaciones de los contratos se 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:

No Aplica

## Fraude y Corrupción

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

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

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

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

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

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

Fraude y corrupción comprenden actos como:

(i) Ofrecer, dar, recibir o solicitar, directa o indirectamente, cualquier cosa de valor para influenciar las acciones de otra parte;

(ii) Cualquier acto u omisión, incluyendo la tergiversación de hechos y circunstancias, que engañen, o intenten engañar, a alguna parte para obtener un beneficio económico o de otra naturaleza o para evadir una obligación;

(iii) Perjudicar o causar daño, o amenazar con perjudicar o causar daño, directa o indirectamente, a cualquier parte o a sus bienes para influenciar las acciones de una parte;

(iv) Colusión o acuerdo entre dos o más partes realizado con la intención de alcanzar un propósito inapropiado, incluyendo influenciar en forma inapropiada las acciones de otra parte.

(v) Cualquier otro acto considerado como tal en la legislación vigente.

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

## **Medio alternativo de Resolución de Conflictos a través del Avenimiento.**

“Los contratistas, proveedores, consultores y contratantes, podrán solicitar la intervención de la Dirección Nacional de Contrataciones Públicas alegando el incumplimiento de los términos y condiciones pactados 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.

