

**PLIEGO DE BASES Y CONDICIONES**

---

Convocante:

**Banco Nacional de Fomento (BNF)**

**Uoc Bnf**

Nombre de la Licitación:

**ADQUISICIÓN DE LICENCIAS SOFTWARE DE  
SOPORTE TÉCNICO - ANTIVIRUS (SBE)**

(versión 4)

ID de Licitación:

**395689**



Modalidad:

**Licitación Pública Nacional**

Publicado el:

**15/03/2022**

*"Pliego para la Adquisición de Bienes y/o Servicios - SBE"*

*Versión 1*

# RESUMEN DEL LLAMADO

## Datos de la Convocatoria

ID de Licitación:	395689	Nombre de la Licitación:	Adquisición de Licencias Software de Soporte Técnico - Antivirus (SBE)
Convocante:	Banco Nacional de Fomento (BNF)	Categoría:	24 - Equipos, accesorios y programas computacionales, de oficina, educativos, de imprenta, de comunicación y señalamiento
Unidad de Contratación:	Uoc Bnf	Tipo de Procedimiento:	LPN - Licitación Pública Nacional

## Etapas y Plazos

Lugar para Realizar Consultas:	Consultas Virtuales a traves del portal	Fecha Límite de Consultas:	22/02/2022 12:00
Lugar de Entrega de Ofertas:	En las oficinas de la GDOC - Casa Matriz del BNF (Independencia Nacional y 25 de Mayo)	Fecha de Entrega de Ofertas:	28/03/2022 09:00
Lugar de Apertura de Ofertas:	En las oficinas de la GDOC - Casa Matriz del BNF (Independencia Nacional y 25 de Mayo)	Fecha de Apertura de Ofertas:	28/03/2022 09:15

## Adjudicación y Contrato

Sistema de Adjudicación:	Por Total	Anticipo:	No se otorgará anticipo
Vigencia del Contrato:	Hasta Cumplimiento Total de Obligaciones		

## Datos del Contacto

Nombre:	CAROLINA AUADA	Cargo:	GERENTE DPTAL. DE CONTRATACIONES
Teléfono:	4191578	Correo Electrónico:	carolinaauada@bnf.gov.py

# ADENDA

## Adenda

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

### ADENDA N° 3

Señores

..

Presente:

Tenemos el agrado de dirigirnos a ustedes, con relación a la Licitación Pública Nacional BNF LPN SBE N° 6/2022 para la **Adquisición de Licencias Software de Soporte Técnico - Antivirus (SBE) ID N° 395.689.-**

Al respecto, cumplimos en informar que se realizan modificaciones en el Pliego de Bases y Condiciones, conforme se indican a continuación:

#### v. Requisitos de Calificación y Criterios de Evaluación - Capacidad Técnica:

#### **Capacidad Técnica**

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

1. Contar con 3 (tres) personales técnicos en su plantel, del producto ofertado en la presente licitación.

1.1. El oferente deberá contar con Personal Técnico que en su conjunto posean las siguientes certificaciones:

- Como mínimo 2 (dos) Técnicos Certificados en Professional: Endpoint Security for Windows SP.
- Como mínimo 2 (dos) técnicos certificados en Systems Engineer Level 1.
- Como mínimo 2 (dos) técnicos certificados en Professional: Encryption.
- Como mínimo 2 (dos) técnicos certificados en Professional: Systems Management
- Como mínimo 2 (dos) técnicos certificados en Kaspersky Security 9.0 for Microsoft Exchange Servers.
- Contar un mínimo de 3 (tres) técnicos capacitados y certificados por la marca del Antivirus KASPERSKY ofertada en la presente licitación.
- Contar con una estructura, soporte y Asistencia telefónica de 24 horas
- Contar como mínimo con 3 ingenieros certificados con las certificaciones avanzadas del producto.
- Contar como mínimo con 2 técnicos con certificaciones de cifrado a fin de instalar y configurar correctamente los módulos de cifrado.
- Contar con por lo menos 2 técnicos con certificaciones en protección de servidores de correo antispam a fin de garantizar la correcta instalación y configuración del servidor antispam.
- Contar por lo menos con 2 técnicos con certificaciones en Detección y Respuesta de Endpoints (EDR) a fin de garantizar el correcto despliegue y configuración de los módulos EDR
- Contar por lo menos con 2 técnicos con certificaciones en soluciones de protección para entornos híbridos o virtualizados a fin de garantizar la correcta implementación de los appliances virtuales para proteger los entornos virtualizados de los desktops.
- Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar **planilla de IPS y/o certificados de inscripción en IPS**
- Contar como mínimo con 2 ingenieros con certificaciones ITIL para garantizar la buena asistencia en soporte técnico.

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

#### v. Requisitos de Calificación y Criterios de Evaluación - Requisitos documentales para evaluar el criterio de capacidad técnica:

1. Presentar Declaración Jurada donde se indique que la empresa oferente, cuenta con 3 (tres) personales técnicos en

su plantel, del producto ofertado en la presente licitación.

1. El oferente deberá contar con Personal Técnico que en su conjunto posean las siguientes certificaciones:

- Como mínimo 2 (dos) Técnicos Certificados en Professional: Endpoint Security for Windows SP. (Presentar Certificado)
- Como mínimo 2 (dos) técnicos certificados en Systems Engineer Level 1. (Presentar Certificado)
- Como mínimo 2 (dos) técnicos certificados en Professional: Encryption. (Presentar Certificado)
- Como mínimo 2 (dos) técnicos certificados en Professional Systems Management (Presentar Certificado)
- Como mínimo 2 (dos) técnicos certificados en Kaspersky Security 9.0 for Microsoft Exchange Servers. (Presentar Certificado)
- Declaración jurada de disponer un mínimo de 3 (tres) técnicos capacitados y certificados por la marca del Antivirus KASPERSKY ofertada en la presente licitación.
- Presentar Declaración Jurada donde manifieste que posee una estructura, soporte y Asistencia telefónica de 24 horas.
- Contar como mínimo con 3 ingenieros certificados con las certificaciones avanzadas del producto - (Presentar Certificado)
- Contar como mínimo con 2 técnicos con certificaciones de cifrado a fin de instalar y configurar correctamente los módulos de cifrado - (Presentar Certificado)
- Contar con por lo menos 2 técnicos con certificaciones en protección de servidores de correo antispam a fin de garantizar la correcta instalación y configuración del servidor antispam - (Presentar Certificado)
- Contar por lo menos con 2 técnicos con certificaciones en Detección y Respuesta de Endpoints (EDR) a fin de garantizar el correcto despliegue y configuración de los módulos EDR (Presentar Certificado)
- Contar por lo menos con 2 técnicos con certificaciones en soluciones de protección para entornos híbridos o virtualizados a fin de garantizar la correcta implementación de los appliances virtuales para proteger los entornos virtualizados de los desktops - (Presentar Certificado)
- Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar **planilla de IPS y/o certificados de inscripción en IPS**
- Contar como mínimo con 2 ingenieros con certificaciones ITIL para garantizar la buena asistencia en soporte técnico - (Presentar Certificado).

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

***Todos los demás requisitos establecidos en el Pliego de Bases y Condiciones permanecen sin variación.***

**v. Suministros Requeridos Especificaciones Técnicas Detalles de los productos y/o servicios con las respectivas especificaciones técnicas:**

**14. Términos a tener en cuenta:**

14.1. El proveedor deberá incluir con la propuesta un curso de Ciberseguridad, con una carga horaria de 12 horas como mínimo para tres personas, incluyendo los siguientes puntos.

14.1.1. Seguridad en entornos Windows y GNU/Linux.

14.1.2. Estrategias de Defensa.

14.1.3. Definición de políticas de Seguridad en la Institución.

14.2. Contar como mínimo con 3 profesionales certificados como Kaspersky KL Certified Professional o superior.

14.3. Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar **planilla de IPS y/o certificados de inscripción en IPS.**

14.4. Contar con 10 contratos o facturas de la provisión del Software ofertado entre los años 2018, 2019 y 2020.

14.5. Implementación de todos los módulos de la herramienta en todo el parque de equipos.

14.6. Capacitación de la herramienta a todas las personas involucradas en el departamento de tecnología y de seguridad de la información.

14.7. Soporte técnico prioritario 24x7 con tiempo de respuesta inferior a 3 horas para Asunción y 24 horas para el interior del país incluido durante todo el periodo de licenciamiento.

14.8. Cantidad de tickets de soporte ilimitados.

*Todos los demás requisitos establecidos en el Pliego de Bases y Condiciones permanecen sin variación.*

Se detectaron modificaciones en las siguientes cláusulas:

Sección: Requisitos de calificación y criterios de evaluación

- Capacidad Técnica
- Requisitos documentales para evaluar el criterio de capacidad técnica

Sección: Suministros requeridos - especificaciones técnicas

- Detalles de los productos y/o servicios con las respectivas especificaciones técnicas - CPS

Se puede realizar una comparación de esta versión del pliego con la versión anterior en el siguiente enlace:

<https://www.contrataciones.gov.py/licitaciones/convocatoria/395689-adquisicion-licencias-soporte-tecnico-antivirus-sbe-ad-referendum-2022-1/pliego/4/diferencias/3.html?seccion=adenda>

La adenda es el documento emitido por la convocante, mediante la cual se modifican aspectos establecidos en la convocatoria y/o en las bases de la licitación o en los contratos suscriptos. La adenda será considerada parte integrante del documento cuyo contenido modifique.

# DATOS DE LA LICITACIÓN

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.

## Contratación Pública Sostenible - CPS

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

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

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

Criterios sociales y económicos:

- Los oferentes deberán indicar bajo declaración jurada el pago del salario mínimo a sus colaboradores, además de garantizar la no contratación de menores.
- Los oferentes deberán dar cumplimiento a las disposiciones legales vigentes asegurando a los trabajadores dependientes condiciones de trabajo dignas y justas en lo referente al salario, cargas sociales, provisión de uniformes, provisión de equipos de protección individual, bonificación familiar, jornada laboral, asegurar condiciones especiales a trabajadores expuestos a trabajos insalubres y peligrosos, remuneración por jornada nocturna.
- Las deducciones al salario, anticipos y préstamos a los trabajadores no podrán exceder los límites legales. Los términos y condiciones relacionados a los mismos deberán comunicarse de manera clara, para que los trabajadores los entiendan.
- Los oferentes adjudicados deberán fomentar en la medida de lo posible, la creación de empleo local y el uso de suministros locales.

Criterios ambientales:

- El oferente adjudicado deberá utilizar en la medida de lo posible, insumos cuyo embalaje pueda ser reutilizado o reciclado.
- El oferente adjudicado deberá cumplir con los lineamientos ambientales, incluidos en el ordenamiento jurídico o dictado por la institución, tales como: cooperación en acciones de recolección, separación de residuos sólidos, disposición adecuada de los residuos, participación del personal en actividades de capacitación impartidas por la institución, entre otros.
- El oferente adjudicado deberá asegurar que todos los residuos generados por sus actividades sean adecuadamente gestionados (identificados, segregados y destinados) y buscar su reducción o eliminación en la fuente, por medio de prácticas como la modificación de los procesos de producción, manutención y de las instalaciones utilizadas, además de la sustitución, conservación, reciclaje o reutilización de materiales.

Conducta empresarial responsable:

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

- No ofrecer, prometer, dar ni solicitar, directa o indirectamente, pagos ilícitos u otras ventajas indebidas para obtener o conservar un contrato u otra ventaja ilegítima.
- No ofrecer, prometer o conceder ventajas indebidas, pecuniarias o de otro tipo a funcionarios públicos. Tampoco deberán solicitar, recibir o aceptar ventajas indebidas, pecuniarias o de otro tipo, de funcionarios públicos o empleados de sus socios comerciales.
- Introducir políticas y programas contra la corrupción e implementarlas dentro de sus operaciones.
- Garantizar que todos los recursos a ser empleados en la ejecución de un contrato público sean de origen lícito.
- Garantizar que los fondos obtenidos de una licitación pública no sean destinados a fines ilícitos.

---

## **Difusión de los documentos de la licitación**

Todos los datos y documentos de esta licitación deben ser obtenidos directamente del Sistema de Información de Contrataciones Públicas (SICP). Es responsabilidad del oferente examinar todos los documentos y la información de la licitación que obre en el mismo.

---

## **Aclaración de los documentos de la licitación**

Todo oferente potencial que necesite alguna aclaración del pliego de bases y condiciones podrá solicitarla a la convocante. El medio por el cual se recibirán las consultas es el Sistema de Información de Contrataciones Públicas (SICP), y/o si es el caso, en la Junta de Aclaraciones que se realice en la fecha, hora y dirección indicados por la convocante.

La convocante responderá por escrito a toda solicitud de aclaración del PBC que reciba dentro del plazo establecido que se derive de la Junta de Aclaraciones.

La convocante publicará su respuesta incluida una explicación de la consulta, pero sin indentificar su procedencia, a través del SICP, dentro del plazo tope.

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

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.

---

## **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 Sistema de Información de Proveedores del Estado (SIPE) de la DNCP, podrán presentar con su oferta, la constancia firmada emitida a través del SIPE, que reemplazará a los documentos solicitados por la convocante en el presente pliego.

Los oferentes deberán indicar en su oferta, qué documentos que forman parte de la misma son de carácter confidencial 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.

---

## **Oferentes en consorcio**

Dos o más interesados que no se encuentren comprendidos en las inhabilidades para presentar ofertas o contratar, podrán unirse temporalmente para presentar una oferta sin crear una persona jurídica.

Para ello deberán presentar escritura pública de constitución del consorcio o un acuerdo con el compromiso de formalizar el consorcio 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.

## **Aclaración de las ofertas**

Con el objeto de facilitar el proceso de revisión, evaluación, comparación y posterior calificación de ofertas, el Comité de Evaluación solicitará 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 al pliego de bases y condiciones, 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 establecido por el mismo, 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:

1. 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 total y el precio unitario será corregido.
2. Los precios subtotales podrán ser corregidos siempre que se mantenga inalterable el precio total obtenido en la SBE.
3. En ambos casos, los precios unitarios modificados no podrán ser superiores a los precios unitarios iniciales que figuran en el Acta de Sesión Pública Virtual de la SBE.
4. En caso de que el oferente haya cotizado su precio en guaraníes con décimos y céntimos, la convocante procederá a realizar el redondeo hacia abajo, aún cuando el resultado varíe del precio total que se encuentra en el Acta de Sesión Pública Virtual de la SBE como precio final.
5. 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 (1) y (2) mencionados.

---

## Idioma de la oferta

La oferta deberá ser presentada en idioma castellano o en su defecto acompañado de su traducción oficial, realizada por un traductor público matriculado en la República del Paraguay.

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

No Aplica

---

## Idioma del contrato

El contrato, así como toda la correspondencia y documentos relativos al contrato, deberán ser escritos en idioma castellano. Los documentos de sustento y material impreso que formen parte del contrato, pueden estar redactados en otro idioma siempre que estén acompañados de una traducción realizada por traductor matriculado en la República del Paraguay, en sus partes pertinentes al idioma castellano y, en tal caso, dicha traducción prevalecerá para efectos de interpretación del contrato.

El proveedor correrá con todos los costos relativos a las traducciones, así como todos los riesgos derivados de la exactitud de dicha traducción.

---

## Moneda de la oferta y pago

La moneda de la oferta y pago será:

En Guaraníes para todos los oferentes

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

---

## Visita al sitio de ejecución del contrato

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

No Aplica

Al culminar la o las visitas, se labrará acta en la cual conste, la fecha, lugar y hora de realización, en la cual se identifique el nombre de las personas que asistieron en calidad de potenciales oferentes, así como del funcionario encargado de dicho acto.

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

Cuando la convocante haya establecido que no será requisito de participación, el oferente podrá declarar bajo fe de juramento conocer el sitio y que cuenta con la información suficiente para preparar la oferta y ejecutar el contrato.

---

## **Precio y formulario de la oferta**

El oferente indicará el precio total de su oferta y los precios unitarios de los bienes 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.

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 requeridos, el oferente deberá cotizar en la lista de precios todos los ítems, con sus precios unitarios y totales correspondientes.

c) En el caso del sistema de adjudicación por lotes, el oferente cotizará en la lista de precios uno o más lotes, e indicará todos los ítems del lote ofertado con sus precios unitarios y totales correspondientes. En caso de no cotizar uno o más lotes, los lotes no cotizados no requieren ser incorporados a la planilla de precios.

d) En el caso del sistema de adjudicación por ítems, el oferente podrá ofertar por uno o más ítems, en cuyo caso deberá cotizar el precio unitario y total de cada uno o más ítems, los ítems no cotizados no requieren ser incorporados a la planilla de precios.

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

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

3. En caso de indicarse en el SICP, que se utilizará la modalidad de contrato abierto, cuando se realice por montos mínimos y máximos deberán indicarse el precio unitario de los bienes 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 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.

---

## **Abastecimiento simultáneo**

El sistema de abastecimiento simultáneo para esta licitación será:

No Aplica

---

## 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 productos a los cuales se les requerirá Autorización del Fabricante son los indicados a continuación:

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

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

---

## Muestras

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

No Aplica

## **Copias de la oferta - CPS**

El oferente presentará su oferta original. En caso de que la convocante requiera la presentación de copias lo deberá indicar en este apartado, las copias deberán estar identificadas como tales.

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

Cantidad de copias requeridas:

1 copia

## **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.

## **Periodo de validez de las ofertas**

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

90

Las ofertas deberán permanecer válidas por el periodo indicado en el presente apartado, que se computará a partir del inicio de la etapa competitiva. 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 pedirá ni permitirá que modifiquen sus ofertas.

## **Garantías: instrumentación, plazos y ejecución.**

1. La garantía de mantenimiento de oferta deberá expedirse en un monto en guaraníes que no deberá ser inferior al porcentaje especificado en el SICP. El oferente puede adoptar cualquiera de las formas de instrumentación de las garantías dispuestas por las normativas vigentes.
2. La garantía de mantenimiento de oferta presentada en los términos del párrafo anterior, deberá cubrir el precio total de la oferta en la etapa de recepción de propuestas.
3. En los contratos abiertos, el porcentaje de las garantías a ser presentado por los oferentes que participen, deberá ser aplicado sobre el monto máximo total de la oferta; si la adjudicación fuese por lote o ítem ofertado, deberán sumarse los valores máximos de cada lote o ítem ofertado, a fin de obtener el monto sobre el cual se aplicará el porcentaje de la citada garantía.
4. En caso de instrumentarse a través de Garantía Bancaria, deberá estar sustancialmente de acuerdo con el formulario de Garantía de Mantenimiento de Oferta incluido en la Sección "Formularios".
5. La garantía de mantenimiento de oferta en caso de oferentes en consorcio deberá ser presentado de la siguiente manera:
  - Consorcio constituido por escritura pública: deberán emitir a nombre del consorcio legalmente constituido por escritura pública, del líder del consorcio o de todos los socios que la integran;
  - Consorcio en proceso de formación con acuerdo de intención: deberán emitir a nombre del líder del consorcio en proceso de formación con acuerdo de intención o de todos los miembros que la integran.
6. 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 la oferta;
  - c) Si no acepta la corrección aritmética del precio de su oferta, en caso de existir;
  - d) Si el oferente no presentare su oferta en la fecha y hora señaladas, previo requerimiento por parte de la convocante; o
  - e) Si el adjudicatario no procede, por causa imputable al mismo a:
    - e.1. Suministrar los documentos indicados en el pliego de bases y condiciones para la firma del contrato,
    - e.2. Firmar el contrato,
    - e.3. Suministrar en tiempo y forma la garantía de cumplimiento de contrato,
    - e.4. Se comprobare que las declaraciones juradas presentadas por el oferente adjudicado con su oferta sean falsas,
    - e.5. El adjudicatario no presentare las legalizaciones correspondientes para la firma del contrato, cuando éstas sean requeridas, o
    - e.6. No se formaliza el consorcio por escritura pública, antes de la firma del contrato.
7. 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 póliza. 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.
8. 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 cumplimiento deberá ser entregada antes del cumplimiento de la prestación.
9. La garantía de Fiel Cumplimiento de Contrato será liberada y devuelta al proveedor, a requerimiento de parte, a más tardar treinta (30) días contados a partir de la fecha de cumplimiento de las obligaciones del proveedor en virtud de contrato, incluyendo cualquier obligación relativa a la garantía de los bienes.

## **Periodo de Validez de la Garantía de Mantenimiento de Oferta**

El plazo de validez de la Garantía de Mantenimiento de Oferta (en días corridos) 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. Cuando la competencia se desarrolle por más de un día, la garantía de mantenimiento de oferta deberá cubrir a partir del primer día del inicio de la etapa competitiva.

---

## Porcentaje de Garantía de Fiel Cumplimiento de Contrato

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

10,00 %

La garantía de Fiel Cumplimiento de Contrato deberá ser presentada por el proveedor, dentro de los diez (10) días calendario siguientes a partir de la fecha de suscripción del contrato, de conformidad con lo dispuesto en el artículo 39 de la Ley N° 2051/2003.

---

## Periodo de Validez de la Garantía de Fiel Cumplimiento de Contrato

El plazo de vigencia de la Garantía de Fiel Cumplimiento de Contrato será de:

- Desde la suscripción del contrato hasta 30 días posteriores contados a partir de su finalización (cumplimiento total a satisfacción de la Convocante).

---

## Periodo de validez de la garantía de los bienes

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

No Aplica

---

## Tiempo de funcionamiento de los bienes

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

No Aplica

---

## **Plazo de reposición de bienes**

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

No Aplica

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

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

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

2. Si el proveedor después de haber sido notificado, no cumple con su obligación dentro del plazo establecido, la contratante tomará las 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.

---

## **Cobertura de seguro de los bienes**

La cobertura de seguro requerida a los bienes será:

No Aplica

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

---

## **Sistema de presentación de ofertas**

Las ofertas serán presentadas en un sólo sobre y deberán:

1. Indicar el nombre y la dirección del oferente;
2. Estar dirigidos a la convocante;
3. Llevar la identificación específica del proceso de licitación indicado en el SICP; y

4. Llevar una advertencia de no abrir antes de la hora y fecha de apertura de ofertas.

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.

## **Plazo para presentar las ofertas**

Culminada la etapa competitiva, presentarán las ofertas físicas en la dirección y hasta la fecha y hora que se indican en el SICP, los siguientes participantes requeridos:

Todos los oferentes

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

La convocante podrá a su discreción, extender el plazo originalmente establecido para la presentación de ofertas mediante una adenda. 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.

## **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.

## **Apertura de ofertas**

1. La convocante abrirá las ofertas y en caso de que hubiere notificaciones de retiro, sustitución y modificación de ofertas

presentadas, las leerá en el acto público con la presencia de los oferentes o sus representantes a la hora, en la fecha y el lugar establecidos en el SICP.

2. Cuando la presentación de oferta sea electrónica, el acto de apertura deberá sujetarse a la reglamentación vigente, en la fecha, hora y lugar establecidos en el SICP.
3. Primero se procederá a verificar de entre las ofertas recibidas por courier o entregadas personalmente, los sobres 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 pertinente contenga la autorización válida para solicitar el retiro 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 ninguna sustitución a menos que la comunicación de sustitución correspondiente contenga una autorización válida para solicitar la sustitución 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 correspondiente contenga la autorización válida para solicitar la modificación 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 los documentos que soliciten, 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 portado por el representante.
5. Se solicitará a los representantes de los oferentes que estén presentes que firmen el acta. La omisión de la firma por parte de un oferente no invalidará el contenido y efecto del acta. Se distribuirá una copia del acta a todos los presentes.
6. Las ofertas sustituidas y modificadas presentadas, 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 oferentes 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.
8. El acta de apertura deberá ser comunicada al SICP, para su difusión, dentro de los dos (02) días hábiles de la realización del acto de apertura.

# REQUISITOS DE CALIFICACIÓN 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 ésta licitación, individualmente o en forma conjunta (consorcio), los oferentes domiciliados en la República del Paraguay, que no se encuentren comprendidos en las prohibiciones o limitaciones para presentar propuestas y contratar con el Estado, establecidas en la Ley N° 2051/03 "De Contrataciones Públicas".

Adicionalmente a lo establecido en el párrafo anterior el oferente deberá considerar las siguientes condiciones de participación:

Que se encuentren registrados/as en el Sistema de Información de Proveedores del Estado (SIPE), debiendo suscribir ante el mismo una Declaración Jurada en la cual manifiesta que tiene pleno conocimiento y acepta las reglas del proceso, para su activación como oferente. La Declaración Jurada referida, podrá ser descargada desde el SICP, módulo del SIPE.

Que activados/as conforme al SIPE posean su Usuario y Contraseña, personal e intransferible, salvo que los mismos hayan sido cancelados por el sistema, de conformidad a la reglamentación específica. La pérdida del usuario y contraseña deberá ser comunicada a la DNCP para que, a través del sistema, sea bloqueado el acceso inmediatamente; y

Como requisito para la participación en la Subasta a la Baja Electrónica, el oferente deberá manifestar en el campo previsto en el sistema electrónico, que cumple plenamente los requisitos de habilitación y que su propuesta de precios está conforme con las exigencias del pliego de bases y condiciones.

## Requisitos de Calificación

### Calificación Legal

Los oferentes deberán declarar que no se encuentran comprendidos en las limitaciones o prohibiciones para contratar con el Estado, contempladas en el artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021, declaración que forma parte del formulario de oferta.

Serán desechadas las ofertas de los oferentes que se encuentren comprendidos en las prohibiciones o limitaciones para contratar 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 los incisos a) y b), m) y n) del artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021, el comité de evaluación realizará el siguiente análisis:

1. Verificará que el oferente haya proporcionado el formulario de ofertas que incluye la declaratoria debidamente firmada.
2. Verificará los registros del personal de la convocante para detectar si el oferente o sus representantes, se hallan comprendidos en el presupuesto del inciso a) del artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021.
3. Verificará por los medios disponibles, si el oferente y los demás sujetos individualizados en las prohibiciones o limitaciones contenidas en los incisos a) y b), m) y n) del artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021, aparecen en la base de datos del SINARH o de la Secretaría de la Función Pública.
4. Si se constatará que alguno de las personas mencionadas en el párrafo anterior figura en la base de datos del SINARH o de la Secretaría de la Función Pública, 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 Miembros, de conformidad a estándar debidamente firmado en su oferta y cotejará los datos con las personas físicas inhabilitadas que constan en el registro de “Sanciones a Proveedores” del SICP a fin de detectar si directores, gerentes, socios gerentes, quienes ejerzan la administración, accionistas, cuotapartistas o propietarios se hallan comprendidos en el presupuesto del inciso m) y n) del artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021.

El comité podrá recurrir a fuentes públicas o privadas de información, para verificar los datos proporcionados por el oferente.

6. Si el Comité confirma que el oferente o sus integrantes poseen impedimentos, la oferta será rechazada y se remitirán los antecedentes a la Dirección Nacional de Contrataciones Públicas (DNCP) para los fines pertinentes.

## **Análisis de precios ofertados**

Durante la evaluación de ofertas, 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 a los siguientes parámetros:

1. 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.

## **Certificado de Producto y Empleo Nacional - CPS**

A los efectos de acogerse al beneficio de la aplicación del margen de preferencia, el oferente deberá contar con el Certificado de Producto y Empleo Nacional (CPEN). El certificado debe ser emitido como máximo a la fecha y hora tope de la etapa competitiva.

La falta del CPEN no será motivo de descalificación de la oferta, sin embargo, el oferente no podrá acogerse al beneficio.

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

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

1. 1. Consorcios:

### **a.1. Provisión de Bienes**

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

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

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

Todos los integrantes del consorcio deben contar con el CPEN.

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

## **Margen de Preferencia Local - CPS**

Para contrataciones realizadas por Unidades Operativas que se encuentren conformadas dentro de un municipio o departamento se deberá considerar que, si la oferta evaluada como la más baja pertenece a una firma u empresa domiciliada fuera del territorio departamental de la convocante, ésta será comparada con la oferta más baja de la firma u empresa domiciliada dentro del territorio de la convocante, agregándole al precio total de la oferta propuesta por la primera una suma del diez por ciento (10%) del precio. Si en dicha comparación adicional la oferta de la firma u empresa domiciliada dentro del territorio departamental de la convocante resultare ser la más baja, se la seleccionará para la adjudicación; en caso contrario se seleccionará la oferta de servicios de la firma u empresa domiciliada fuera del territorio departamental de la convocante.

En el caso de que el oferente, sea de la zona y además cuente con margen de preferencia, se le aplicará únicamente el margen de este último.

Las convocantes deberán acogerse a las condiciones específicas para la aplicación del Margen de Preferencia Local establecidas en la reglamentación emitida por la DNCP.

## **Requisitos documentales para la evaluación de las condiciones de participación**

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

### **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.]

### **2. Garantía de Mantenimiento de Oferta (\*)**

La garantía de mantenimiento de oferta debe ser extendida, bajo la forma de una garantía bancaria o póliza de seguro de caución.

### **3. Certificado de Cumplimiento con la Seguridad Social. (\*\*)**

### **4. Certificado de Producto y Empleo Nacional, emitido por el MIC, en caso de contar. (\*\*)**

5. Constancia de presentación de la <b>Declaración Jurada de bienes y rentas, activos y pasivos</b> ante la Contraloría General de la República, para los sujetos obligados en el marco de la Ley N° 6355/19, entendiéndose que dicha constancia, para llamados convencionales, debe tener fecha de hasta como máximo la fecha de presentación de la oferta física y para llamados por Subasta a la Baja Electrónica, la fecha de hasta como máximo del inicio de la etapa competitiva. Son sujetos obligados conforme a la Ley, las personas físicas y jurídicas, así como los accionistas, directores, socios gerentes y similares de éstas. (**)
6. Declaración Jurada de Declaración de Miembros, de conformidad con el formulario estándar Sección Formularios (**)
7. Certificado de Cumplimiento Tributario. (**)
8. Patente Comercial del municipio en donde esté asentado el establecimiento principal del oferente. (**)
9. Documentos legales
9.1. Oferentes Individuales. Personas Físicas.
<ul style="list-style-type: none"> <li>• Fotocopia simple de la Cédula de Identidad del firmante de la oferta. (*)</li> </ul>
<ul style="list-style-type: none"> <li>• Constancia de inscripción en el Registro Único de Contribuyentes RUC. (*)</li> </ul>
<ul style="list-style-type: none"> <li>• 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. (*)</li> </ul>
9.2. Oferentes Individuales. Personas Jurídicas.
<ul style="list-style-type: none"> <li>• 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. (*)</li> </ul>
<ul style="list-style-type: none"> <li>• Constancia de Inscripción en el Registro Único de Contribuyentes RUC y fotocopia simple de los Documentos de Identidad de los representantes o apoderados de la Sociedad.</li> </ul>
<ul style="list-style-type: none"> <li>• 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. (*)</li> </ul>

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

### 9.3. Oferentes en Consorcio.

1. 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. (\*)

2. 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). (\*)

3. Fotocopia simple de los documentos que acrediten las facultades de los firmantes del acuerdo de intención de consorciarse. Estos documentos pueden consistir en (\*):

- Un poder suficiente otorgado por escritura pública por cada miembro del consorcio (no es necesario que esté inscripto en el Registro de Poderes); o
- Los documentos societarios de cada miembro del consorcio, que justifiquen la representación del firmante, tales como actas de asamblea y de directorio en el caso de las sociedades anónimas.

4. Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al Consorcio, cuando se haya formalizado el Consorcio. Estos documentos pueden consistir en (\*):

- Un poder suficiente otorgado por escritura pública por la Empresa Líder del consorcio (no es necesario que esté inscripto en el Registro de Poderes); o
- Los documentos societarios de la Empresa Líder, que justifiquen la representación del firmante, tales como actas de asamblea y de directorio en el caso de las sociedades anónimas.

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

**Observación:** *El Margen de Preferencia Local - NO APLICA* considerando que el Banco Nacional de Fomento tiene su domicilio en la ciudad de Asunción, capital de la República del Paraguay, la cual no pertenece a ningún Departamento según el Art. 157 de la Constitución Nacional, por ende el presupuesto o la condición prevista en el Art. 64 del Decreto, en los llamados que realice el Banco Nacional de Fomento no se presenta en ningún caso. Para tal efecto mencionamos las Resoluciones DNCP 306/2021 y 511/2021, para lo que hubiera lugar

*Para los oferentes consorciados: el socio líder y cada socio deberá como mínimo cumplir con los siguientes porcentajes:*

a. CAPACIDAD FINANCIERA	<u>70%</u> del requisito mínimo
b. EXPERIENCIA Y CAPACIDAD TÉCNICA	<u>70%</u> del requisito mínimo
c. CALIFICACIÓN LEGAL	El socio líder y cada socio deberá cumplir con el <u>100%</u> de lo exigido

Los documentos indicados con asterisco (\*) son considerados documentos sustanciales a ser presentados con la oferta.

Los documentos indicados con doble asterisco (\*\*) deberán estar vigentes al inicio de la etapa competitiva para procesos de SBE.

## Capacidad Financiera

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

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

*Deberán cumplir el siguiente parámetro:*

a. Ratio de Liquidez: activo corriente / pasivo corriente

***Deberá ser igual o mayor que 1, en promedio, en los años (2018, 2019 y 2020)***

b. Endeudamiento: pasivo total / activo total

***No deberá ser mayor a 0,80 en promedio, en los años (2018, 2019 y 2020)***

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

***El promedio de los años (2018, 2019 y 2020) no deberá ser negativo***

### **b. Para contribuyente de IRPC/IRE SIMPLE**

*Deberán cumplir el siguiente parámetro:*

Eficiencia: (Ingreso/Egreso)

***Deberá ser igual o mayor que 1, en promedio, en los años (2018, 2019 y 2020)***

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

*Deberán cumplir el siguiente parámetro:*

Eficiencia: (Ingreso/Egreso)

***Deberá ser igual o mayor que 1, en promedio, en los años (2018, 2019 y 2020)***

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

*Deberán cumplir el siguiente parámetro:*

Eficiencia: (Ingreso/Egreso)

***Deberá ser igual o mayor que 1, en promedio, en los años (2018, 2019 y 2020)***

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

**Observación:** Si en alguno de los tres años, o los tres años presentados por la Empresa, su pasivo es igual a 0, se considerará el Ratio de Liquidez igual a 1 y se dará por cumplido el Ratio de Endeudamiento.

Esta salvedad en el PBC hace posible calcular el promedio del índice de liquidez de los 3 (tres) ejercicios analizados, debido a que se otorga un valor que puede ser promediado.

## Requisitos documentales para evaluar el criterio de capacidad financiera

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

- |   |
|---|
| a. Certificado de Cumplimiento Tributario vigente al inicio de la etapa competitiva.  |
| b. Balance General y Cuadro de Estado de Resultados de los tres años (2018, 2019 y 2020) para contribuyente de IRACIS/IRE RG.       |
| c. IVA General de 36 (treinta y seis) meses (2018, 2019 y 2020), para contribuyentes sólo del IVA General.                          |
| d. Formulario 106 IRPC, Formulario 501 IRE Simple de los 3 (tres) años (2018, 2019 y 2020) para contribuyentes del IRPC/IRE SIMPLE. |
| e. Formulario 104 IRP, Formulario 515 IRP-RSP de los 3 (tres) años (2018, 2019 y 2020) para contribuyentes de IRP/IRP-RSP.          |

## Experiencia requerida

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

Demostrar la experiencia en la provisión y/o actualización de Software Kaspersky contando con 10 (diez) contratos y/o facturaciones de venta y/o recepciones finales por un monto equivalente al 25% como mínimo del monto total ofertado en la presente licitación, de los: últimos 3 años (2018, 2019 y 2020)

**3 (tres) Constancias emitidas por empresas Públicas y/o Privadas** en las cuales manifieste que el oferente ha brindado satisfactoriamente el Servicio de provisión y/o actualización de Software Kaspersky, en los últimos 3 (tres) años. (Años: 2018, 2019 y 2020).

**Experiencia en el área:** El oferente deberá demostrar una experiencia mínima de 3 (tres) años de constitución de la empresa, con copia del Acta de Constitución de la Empresa.

## Requisitos documentales para evaluar el criterio de experiencia requerida

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

1. Constancia de RUC emitida por la SET.

- |  |
|--|
| 2. Patente comercial vigente al inicio de la etapa competitiva, del municipio donde esté asentado el establecimiento principal del oferente. |
| 3. Copia de contratos y/o facturaciones y/o recepciones finales que avalen la experiencia requerida.   |
| 4. 3 (tres) Constancias emitidas por empresas Públicas y/o Privadas  |
| 5. Copia del Acta de Constitución de la Empresa  |

## Capacidad Técnica

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

1. Contar con 3 (tres) personales técnicos en su plantel, del producto ofertado en la presente licitación.
  - 1.1. El oferente deberá contar con Personal Técnico que en su conjunto posean las siguientes certificaciones:
    - Como mínimo 2 (dos) Técnicos Certificados en Professional: Endpoint Security for Windows SP.
    - Como mínimo 2 (dos) técnicos certificados en Systems Engineer Level 1.
    - Como mínimo 2 (dos) técnicos certificados en Professional: Encryption.
    - Como mínimo 2 (dos) técnicos certificados en Professional: Systems Management
    - Como mínimo 2 (dos) técnicos certificados en Kaspersky Security 9.0 for Microsoft Exchange Servers.
    - Contar un mínimo de 3 (tres) técnicos capacitados y certificados por la marca del Antivirus KASPERSKY ofertada en la presente licitación.
    - Contar con una estructura, soporte y Asistencia telefónica de 24 horas
    - Contar como mínimo con 3 ingenieros certificados con las certificaciones avanzadas del producto.
    - Contar como mínimo con 2 técnicos con certificaciones de cifrado a fin de instalar y configurar correctamente los módulos de cifrado.
    - Contar con por lo menos 2 técnicos con certificaciones en protección de servidores de correo antispam a fin de garantizar la correcta instalación y configuración del servidor antispam.
    - Contar por lo menos con 2 técnicos con certificaciones en Detección y Respuesta de Endpoints (EDR) a fin de garantizar el correcto despliegue y configuración de los módulos EDR
    - Contar por lo menos con 2 técnicos con certificaciones en soluciones de protección para entornos híbridos o virtualizados a fin de garantizar la correcta implementación de los appliances virtuales para proteger los entornos virtualizados de los desktops.
    - Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar **planilla de IPS y/o certificados de inscripción en IPS**
    - Contar como mínimo con 2 ingenieros con certificaciones ITIL para garantizar la buena asistencia en soporte técnico.

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

## Requisitos documentales para evaluar el criterio de capacidad técnica

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

1. Presentar Declaración Jurada donde se indique que la empresa oferente, cuenta con 3 (tres) personales técnicos en su plantel, del producto ofertado en la presente licitación.

1.1. El oferente deberá contar con Personal Técnico que en su conjunto posean las siguientes certificaciones:

- Como mínimo 2 (dos) Técnicos Certificados en Professional: Endpoint Security for Windows SP. (Presentar Certificado)
- Como mínimo 2 (dos) técnicos certificados en Systems Engineer Level 1. (Presentar Certificado)
- Como mínimo 2 (dos) técnicos certificados en Professional: Encryption. (Presentar Certificado)
- Como mínimo 2 (dos) técnicos certificados en Professional Systems Management (Presentar Certificado)
- Como mínimo 2 (dos) técnicos certificados en Kaspersky Security 9.0 for Microsoft Exchange Servers. (Presentar Certificado)
- Declaración jurada de disponer un mínimo de 3 (tres) técnicos capacitados y certificados por la marca del Antivirus KASPERSKY ofertada en la presente licitación.
- Presentar Declaración Jurada donde manifieste que posee una estructura, soporte y Asistencia telefónica de 24 horas.
- Contar como mínimo con 3 ingenieros certificados con las certificaciones avanzadas del producto - (Presentar Certificado)
- Contar como mínimo con 2 técnicos con certificaciones de cifrado a fin de instalar y configurar correctamente los módulos de cifrado - (Presentar Certificado)
- Contar con por lo menos 2 técnicos con certificaciones en protección de servidores de correo antispam a fin de garantizar la correcta instalación y configuración del servidor antispam - (Presentar Certificado)
- Contar por lo menos con 2 técnicos con certificaciones en Detección y Respuesta de Endpoints (EDR) a fin de garantizar el correcto despliegue y configuración de los módulos EDR (Presentar Certificado)
- Contar por lo menos con 2 técnicos con certificaciones en soluciones de protección para entornos híbridos o virtualizados a fin de garantizar la correcta implementación de los appliances virtuales para proteger los entornos virtualizados de los desktops - (Presentar Certificado)
- Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar **planilla de IPS y/o certificados de inscripción en IPS**
- Contar como mínimo con 2 ingenieros con certificaciones ITIL para garantizar la buena asistencia en soporte técnico - (Presentar Certificado).

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

## **Otros criterios que la convocante requiera**

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

- Presentar Certificado expedido por la Secretaria de la Función Pública, en la cual conste que el mismo no es funcionario público; en caso de personas jurídicas presentar el certificado de los miembros de directorio o socios gerentes.

### **OTROS DOCUMENTOS A PRESENTAR PARA LA FIRMA DEL CONTRATO:**

1. Constancia de presentación de la Declaración Jurada de bienes y rentas, activos y pasivos ante la Contraloría General de la República, para los sujetos obligados en el marco de la Ley N° 6355/19, entendiéndose que dicha constancia, para llamados convencionales, debe tener fecha de hasta como máximo la fecha de presentación de la oferta física y para llamados por Subasta a la Baja Electrónica, la fecha de hasta como máximo del inicio de la etapa competitiva. Son sujetos obligados conforme a la Ley, las personas físicas y jurídicas, así como los accionistas, directores, socios gerentes y similares de éstas.

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

---

## **Criterios de desempate de ofertas**

El vencedor de cada grupo subastado será el oferente que ingresó el menor precio. En los casos de igualdad de precios, queda como vencedor el que lo haya ingresado primero.

Siempre que el criterio de desempate establecido, no sea aplicable, el comité de evaluación determinará cuál de ellas es la mejor calificada para ejecutar el contrato utilizando los criterios dispuestos para el efecto por la DNCP.

**Nota1:** Conforme las disposiciones del Decreto 7781/06, para las Contrataciones con Organismos de la Administración Central, el Oferente que resulte adjudicado, deberá contar con una cuenta corriente y/o caja de ahorro habilitada en un Banco de plaza, o en su defecto, hallarse en condiciones de poder habilitar una cuenta corriente y/o caja de ahorro a su nombre, a fin de poder hacer efectivo el Pago Directo a Proveedores y Acreedores vía acreditación en cuenta bancaria.

---

# 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

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 serán suministrados por el proveedor como si hubiesen sido expresamente mencionados, salvo disposición contraria en el contrato.

Los bienes 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.

## Detalles de los productos y/o servicios con las respectivas especificaciones técnicas - CPS

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

### **Renovación y actualización a versiones avanzadas de CiberSeguridad de Kaspersky** **2.000 licencias nuevas por período de 36 (treinta y seis) meses por cada producto**

Banco Nacional de Fomento cuenta actualmente con la solución Kaspersky Total Security for Business que es una suite de seguridad y control que se encuentra implementada en todo el parque de estaciones de trabajo y servidores.

El motivo del presente llamado nace a raíz de la evolución de las Cyber amenazas y la necesidad y el afán de fortalecer las herramientas actuales y dotar al departamento de seguridad del Banco Nacional de Fomento con soluciones avanzadas de Cyber Seguridad con módulos de EDR (Endpoint Detection and Response) que nos permitirá realizar análisis forenses, respuesta ante incidentes e indicadores de compromiso, servidor de sandbox que permitirá realizar un análisis dinámico y detallado de las Cyber amenazas desconocidas, dirigidas y evasivas, adicionalmente una herramienta de protección para entornos híbridos que nos permitirá proteger los escritorios virtuales

#### **Especificaciones técnicas**

- 1. Servidor de Administración y Consola Administrativa**

## 1.1. Compatibilidad:

1.1.1. Microsoft Windows 10 20H2 32 bits o 64 bits (versiones 12.2 en adelante).

1.1.2. Microsoft Windows 10 20H1 32 bits o 64 bits (versiones 12.1 en adelante).

1.1.3. Microsoft Windows 10 Enterprise 2019 LTSC 32 bits / 64 bits.

1.1.4. Microsoft Windows 10 Enterprise 2016 LTSC 32 bits / 64 bits.

1.1.5. Microsoft Windows 10 Enterprise 2015 LTSC 32 bits / 64 bits.

1.1.6. Microsoft Windows 10 Pro RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits.

1.1.7. Microsoft Windows 10 Pro para estaciones de trabajo RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits.

1.1.8. Microsoft Windows 10 Enterprise RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits.

1.1.9. Microsoft Windows 10 Pro 19H1 32 bits / 64 bits.

1.1.10. Microsoft Windows 10 Pro for Workstations 19H1 32 bits / 64 bits.

1.1.11. Microsoft Windows 10 Enterprise 19H1 32 bits / 64 bits.

1.1.12. Microsoft Windows 10 Pro 19H2 32 bits / 64 bits.

1.1.13. Microsoft Windows 10 Pro for Workstations 19H2 32 bits / 64 bits.

1.1.14. Microsoft Windows 10 Enterprise 19H2 32 bits / 64 bits.

1.1.15. Microsoft Windows 8.1 Pro 32 bits / 64 bits.

1.1.16. Microsoft Windows 8.1 Enterprise 32 bits / 64 bits.

1.1.17. Microsoft Windows 8 Pro 32 bits / 64 bits.

1.1.18. Microsoft Windows 8 Enterprise 32 bits / 64 bits.

1.1.19. Microsoft Windows 7 Professional con Service Pack 1 y versiones posteriores 32 bits / 64 bits.

1.1.20. Microsoft Windows 7 Enterprise / Ultimate con Service Pack 1 y versiones posteriores 32 bits / 64 bits.

1.1.21. Windows Server 2019 Standard 64 bits..

1.1.22. Windows Server 2019 Core 64 bits.

1.1.23. Windows Server 2019 Datacenter 64 bits.

1.1.24. Windows Server 2016 Server Standard RS3 (v1709) (LTSC / CBB) 64 bits.

1.1.25. Windows Server 2016 Server Datacenter RS3 (v1709) (LTSC / CBB) 64 bits.

- 1.1.26. Windows Server 2016 Server Core RS3 (v1709).
- 1.1.27. Windows Server 2016 Standard (LTSB) 64 bits.
- 1.1.28. Windows Server 2016 Server Core.
- 1.1.29. Windows Server 2016 Datacenter (LTSB) 64 bits
- 1.1.30. Windows Server 2012 R2 Standard 64 bits.
- 1.1.31. Windows Server 2012 R2 Server Core 64 bits
- 1.1.32. Windows Server 2012 R2 Datacenter 64 bits.
- 1.1.33. Windows Server 2012 Standard 64 bits.
- 1.1.34. Windows Server 2012 Server Core 64 bits.
- 1.1.35. Windows Server 2012 Datacenter 64 bits.
- 1.1.36. Windows Storage Server 2016 64 bits.
- 1.1.37. Windows Storage Server 2012 R2 64 bits.
- 1.1.38. Windows Storage Server 2012 64 bits.

## **2. Características:**

- 2.1.1. Se debe acceder a la consola vía WEB (HTTPS) o MMC;
- 2.1.2. Compatibilidad con Windows FailoverClustering u otra solución de alta disponibilidad
- 2.1.3. Capacidad de eliminar remotamente cualquier solución antivirus (propia o de terceros) que esté presente en las estaciones y servidores, sin la necesidad de la contraseña de remoción del actual antivirus;
- 2.1.4. Capacidad de instalar remotamente la solución de antivirus en las estaciones y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory;
- 2.1.5. Capacidad de instalar remotamente la solución de seguridad en smartphones y Android, utilizando estaciones como intermediadoras;
- 2.1.6. Capacidad de instalar remotamente la solución de seguridad en smartphones y tablets de sistema iOS;
- 2.1.7. Capacidad de instalar remotamente cualquier app en smartphones y tablets de sistema iOS;;
- 2.1.8. Capacidad de gestionar estaciones de trabajo y servidores de archivos (tanto Windows como Linux) protegidos por la solución antivirus;

- 2.1.9. Capacidad de gestionar smartphones y tablets (Android y iOS) protegidos por la solución antivirus;
- 2.1.10. Capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto;
- 2.1.11. Capacidad de actualizar los paquetes de instalación con las últimas vacunas, para que cuando el paquete sea utilizado en una instalación ya contenga las últimas vacunas lanzadas;
- 2.1.12. Capacidad de hacer distribución remota de cualquier software, o sea, debe ser capaz de remotamente enviar cualquier software por la estructura de gerenciamiento de antivirus para que sea instalado en las máquinas clientes;
- 2.1.13. Capacidad de desinstalar remotamente cualquier software instalado en las máquinas clientes;
- 2.1.14. Capacidad de aplicar actualizaciones de Windows remotamente en las estaciones y servidores;
- 2.1.15. Capacidad de importar la estructura de Active Directory para encontrar máquinas;
- 2.1.16. Capacidad de monitorear diferentes subnets de red con el objetivo de encontrar máquinas nuevas para que sean agregadas a la protección;
- 2.1.17. Capacidad de monitorear grupos de trabajos ya existentes y cualquier grupo de trabajo que sea creado en la red, a fin de encontrar máquinas nuevas para ser agregadas a la protección;
- 2.1.18. Capacidad de, al detectar máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antivirus instalado. En caso de no tenerlo, debe instalar el antivirus automáticamente;
- 2.1.19. Capacidad de agrupamiento de máquinas por características comunes entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antivirus instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 2 días, etc;
- 2.1.20. Capacidad de definir políticas de configuraciones diferentes por grupos de estaciones, permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos;
- 2.1.21. Debe proporcionar las siguientes informaciones de las computadoras:
- 2.1.21.1. Si el antivirus está instalado;
- 2.1.21.2. Si el antivirus ha iniciado;
- 2.1.21.3. Si el antivirus está actualizado;
- 2.1.21.4. Minutos/horas desde la última conexión de la máquina con el servidor administrativo;
- 2.1.21.5. Minutos/horas desde la última actualización de vacunas
- 2.1.21.6. Fecha y horario de la última verificación ejecutada en la máquina;
- 2.1.21.7. Versión del antivirus instalado en la máquina;
- 2.1.21.8. Si es necesario reiniciar la computadora para aplicar cambios;

- 2.1.21.9. Fecha y horario de cuando la máquina fue encendida;
- 2.1.21.10. Cantidad de virus encontrados (contador) en la máquina;
- 2.1.21.11. Nombre de la computadora;
- 2.1.21.12. Dominio o grupo de trabajo de la computadora;
- 2.1.21.13. Fecha y horario de la última actualización de vacunas;
- 2.1.21.14. Sistema operativo con Service Pack;
- 2.1.21.15. Cantidad de procesadores;
- 2.1.21.16. Cantidad de memoria RAM;
- 2.1.21.17. Usuario(s) conectados en ese momento, con información de contacto (si están disponibles en el Active Directory)
- 2.1.21.18. Dirección IP;
- 2.1.21.19. Aplicativos instalados, inclusive aplicativos de terceros, con historial de instalación, conteniendo fecha y hora que el software fue instalado o removido.
- 2.1.21.20. Actualizaciones de Windows Updates instaladas
- 2.1.21.21. Información completa de hardware conteniendo: procesadores, memoria, adaptadores de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD
- 2.1.21.22. Vulnerabilidades de aplicativos instalados en la máquina
- 2.1.22. Debe permitir bloquear las configuraciones del antivirus instalado en las estaciones y servidores de manera que el usuario no consiga modificarlas;
- 2.1.23. Capacidad de reconectar máquinas clientes al servidor administrativo más próximo, basado en reglas de conexión como:
  - 2.1.23.1. Cambio de gateway;
  - 2.1.23.2. Cambio de subnet DNS;
  - 2.1.23.3. Cambio de dominio;
  - 2.1.23.4. Cambio de servidor DHCP;
  - 2.1.23.5. Cambio de servidor DNS;
  - 2.1.23.6. Cambio de servidor WINS;
  - 2.1.23.7. Aparición de nueva subnet;
- 2.1.24. Capacidad de configurar políticas móviles para que cuando una computadora cliente esté fuera de la estructura de protección pueda actualizarse vía internet;
- 2.1.25. Capacidad de instalar otros servidores administrativos para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes;

2.1.26. Capacidad de interrelacionar servidores en estructura de jerarquía para obtener informes sobre toda la estructura de antivirus;

2.1.27. Capacidad de herencia de tareas y políticas en la estructura jerárquica de servidores administrativos;

2.1.28. Capacidad de elegir cualquier computadora cliente como repositorio de vacunas y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red;

2.1.29. Capacidad de hacer de este repositorio de vacunas un gateway para conexión con el servidor de administración, para que otras máquinas que no logran conectarse directamente al servidor puedan usar este gateway para recibir y enviar informaciones al servidor administrativo.

2.1.30. Capacidad de exportar informes para los siguientes tipos de archivos: PDF, HTML y XML.

2.1.31. Capacidad de generar traps SNMP para monitoreo de eventos;

2.1.32. Capacidad de enviar correos electrónicos para cuentas específicas en caso de algún evento;

2.1.33. Debe tener compatibilidad con Microsoft NAP, cuando se instale en Windows 2008 Server;

2.1.34. Debe tener compatibilidad con Cisco Network Admission Control (NAC);

2.1.35. Debe tener documentación de la estructura del banco de datos para generación de informes a partir de herramientas específicas de consulta (CrystalReports, por ejemplo).

2.1.36. Capacidad de conectar máquinas vía Wake on Lan para realización de tareas (barrido, actualización, instalación, etc.), inclusive de máquinas que estén en subnets diferentes del servidor);

2.1.37. Capacidad de habilitar automáticamente una política en caso de que ocurra una epidemia en la red (basado en cantidad de virus encontrados en determinado intervalo de tiempo);

2.1.38. Capacidad de realizar actualización incremental de vacunas en las computadoras clientes;

2.1.39. Capacidad de reportar vulnerabilidades de software presentes en las computadoras.

2.1.40. Capacidad de realizar inventario de hardware de todas las máquinas clientes;

2.1.41. Capacidad de realizar inventario de aplicativos de todas las máquinas clientes;

2.1.42. Capacidad de diferenciar máquinas virtuales de máquinas físicas;

### **3. Estaciones Windows**

#### **3.1. Compatibilidad:**

##### **3.1.1. Windows 10**

3.1.2. Windows 8.1

3.1.3. Windows 8

3.1.4. Windows 7 todas las versiones, Service Pack 1 o superior

### 3.2. Características:

3.2.1. Debe proporcionar las siguientes protecciones:

3.2.1.1. Antivirus de archivos residente (antispymware, antitroyano, antimalware, antiransomware, análisis de comportamiento y detección de anomalías, etc.) que verifique cualquier archivo creado, accedido o modificado;

3.2.1.2. Antivirus de web (módulo para verificación de sitios y downloads contra virus)

3.2.1.3. Antivirus de correo electrónico (módulo para verificación de correos recibidos y enviados, así como sus adjuntos)

3.2.1.4. Antivirus de mensajes instantáneos (módulo para verificación de mensajes instantáneos, como ICQ, MSN, IRC, etc)

3.2.1.5. Firewall con IDS

3.2.1.6. Autoprotección (contra ataques a los servicios/procesos del antivirus)

3.2.1.7. Control de dispositivos externos

3.2.1.8. Control de acceso a sitios por categoría

3.2.1.9. Control de ejecución de aplicativos

3.2.1.10. Control de vulnerabilidades de Windows y de los aplicativos instalados

3.2.2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota;

3.2.3. Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo).

3.2.4. Capacidad de automáticamente deshabilitar el Firewall de Windows (en caso de que exista) durante la instalación, para evitar incompatibilidad con el Firewall de la solución;

3.2.5. Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación;

3.2.6. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, (ej.: Win32.Trojan.banker) para que cualquier objeto detectado con el resultado elegido sea ignorado;

3.2.7. Capacidad de agregar aplicativos a una lista de aplicativos confiables, donde las actividades de red, actividades de disco y acceso al registro de Windows no serán monitoreadas;

3.2.8. Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks);

3.2.9. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;

3.2.10. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;

3.2.11. Capacidad de verificar solamente archivos nuevos y modificados;

3.2.12. Capacidad de verificar objetos usando heurística;

3.2.13. Capacidad de agendar una pausa en la verificación;

3.2.14. Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo;

3.2.15. El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe:

3.2.15.1. Preguntar qué hacer, o;

3.2.15.2. Bloquear el acceso al objeto;

3.2.15.2.1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador);

3.2.15.2.2. Caso positivo de desinfección::

3.2.15.2.2.1. Recuperar el objeto para uso;

3.2.15.2.3. Caso negativo de desinfección:

3.2.15.2.3.1. Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador);

3.2.16. Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto.

3.2.17. Capacidad de verificar correos electrónicos recibidos y enviados en los protocolos POP3, IMAP, NNTP, SMTP y MAPI, así como conexiones cifradas (SSL) para POP3 y IMAP (SSL);

3.2.18. Capacidad de verificar tráfico de ICQ, MSN, AIM y IRC contra virus y enlaces phishings;

3.2.19. Capacidad de verificar enlaces introducidos en correos electrónicos contra pishings;

3.2.20. Capacidad de verificar tráfico SSL en los browsers: Internet Explorer, Firefox y Opera;

3.2.21. Capacidad de verificación del cuerpo del correo electrónico y adjuntos usando heurística;

3.2.22. El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe::

3.2.22.1. Preguntar qué hacer, o;

3.2.22.2. Bloquear el correo electrónico;

3.2.22.2.1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador);

3.2.22.2.2. Caso positivo de desinfección:

3.2.22.2.2.1. Recuperar el correo electrónico al usuario;;

3.2.22.2.3. Caso negativo de desinfección:

3.2.22.2.3.1. Mover a cuarentena o borrar el objeto (de acuerdo con la configuración preestablecida por el administrador);

3.2.23. En caso de que el correo electrónico contenga código que parece ser, pero no es definitivamente malicioso, este debe mantenerse en cuarentena.

3.2.24. Posibilidad de verificar solamente correos electrónicos recibidos, o recibidos y enviados.

3.2.25. Capacidad de filtrar adjuntos de correos electrónicos, borrándolos o renombrándolos de acuerdo con la configuración hecha por el administrador.

3.2.26. Capacidad de verificación de tráfico HTTP y cualquier script de Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;

3.2.27. Debe tener soporte total al protocolo IPv6;

3.2.28. Capacidad de modificar las puertas monitoreadas por los módulos de web y correo electrónico;

3.2.29. En la verificación de tráfico web, en caso de que se encuentre código malicioso el programa debe:

3.2.29.1. Preguntar qué hacer, o;

3.2.29.2. Bloquear el acceso al objeto y mostrar un mensaje sobre el bloqueo, o;

3.2.29.3. Permitir acceso al objeto;

3.2.30. El antivirus de web debe realizar la verificación de, como mínimo, dos maneras diferentes, a elección del administrador:

3.2.30.1. Verificación on-the-fly, donde los datos se verifican mientras son recibidos en tiempo real, o;

3.2.30.2. Verificación de buffer, donde los datos se reciben y son almacenados para posterior verificación.

3.2.31. Posibilidad de agregar sitios de la web en una lista de exclusión, donde no serán verificados por el antivirus de web.

3.2.32. Debe contar con módulo que analice las acciones de cada aplicación en ejecución en la computadora, grabando las acciones ejecutadas y comparándolas con secuencias características de actividades peligrosas. Tales registros de secuencias deben ser actualizados conjuntamente con las vacunas.

3.2.33. Debe contar con módulo que analice cada macro de VBA ejecutado, buscando señales de actividad maliciosa.

3.2.34. Debe contar con módulo que analice cualquier intento de edición, exclusión o grabación del registro, de forma que sea posible elegir claves específicas para ser monitoreadas y/o bloqueadas.

3.2.35. Debe tener módulo de bloqueo de Phishing, con actualizaciones incluidas en las vacunas, obtenidas por Anti-PhishingWorkingGroup (<http://www.antiphishing.org/>).

3.2.36. Capacidad de distinguir diferentes subnets y brindar opción de activar o no el firewall para una subnet específica;

3.2.37. Debe tener módulo IDS (IntrusionDetectionSystem) para protección contra portscans y exploración de vulnerabilidades de software. La base de datos de análisis debe actualizarse conjuntamente con las vacunas.

3.2.38. El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:

3.2.38.1. Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas;

3.2.38.2. Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados.

3.2.39. Debe tener módulo que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínimo:

3.2.39.1. Discos de almacenamiento locales

3.2.39.2. Almacenamiento extraíble

3.2.39.3. Impresoras

3.2.39.4. CD/DVD

3.2.39.5. Drives de disquete

3.2.39.6. Modems

3.2.39.7. Dispositivos de cinta

3.2.39.8. Dispositivos multifuncionales

3.2.39.9. Lectores de smart card

3.2.39.10. Dispositivos de sincronización vía ActiveSync (Windows CE, Windows Mobile, etc.)

3.2.39.11. Wi-Fi

3.2.39.12. Adaptadores de red externos

3.2.39.13. Dispositivos MP3 o smartphones

3.2.39.14. Dispositivos Bluetooth

3.2.40. Capacidad de liberar acceso a un dispositivo específico y usuarios específicos por un período de tiempo específico, sin la necesidad de deshabilitar la protección, sin deshabilitar el gerenciamento central o de intervención local del administrador en la máquina del usuario.

3.2.41. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por usuario.

3.2.42. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por agendamiento.

3.2.43. Capacidad de configurar nuevos dispositivos por Class ID/Hardware ID

3.2.44. Capacidad de limitar el acceso a sitios de internet por categoría, por contenido (video, audio, etc.), con posibilidad de configuración por usuario o grupos de usuarios y agendamiento.

3.2.45. Capacidad de limitar la ejecución de aplicativos por hash MD5, nombre del archivo, versión del archivo, nombre del aplicativo, versión del aplicativo, fabricante/desarrollador, categoría (ej.: navegadores, gerenciador de download, juegos, aplicación de acceso remoto, etc.).

3.2.46. Capacidad de bloquear la ejecución de un aplicativo que esté en almacenamiento externo.

3.2.47. Capacidad de limitar el acceso de los aplicativos a recursos del sistema, como claves de registro y carpetas/archivos del sistema, por categoría, fabricante o nivel de confianza del aplicativo.

3.2.48. Capacidad de, en caso de epidemia, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.

3.2.49. Capacidad de, en caso de que la computadora cliente salga de la red corporativa, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.

#### **4. Estaciones de Trabajo y Servidores Linux**

##### **4.1. Compatibilidad:**

4.1.1. Debian GNU / Linux

4.1.2. Ubuntu Server

4.1.3. SuSe Enterprise Linux

4.1.4. RedHat Enterprise Linux

##### **4.2. Características:**

4.2.1. Debe proporcionar las siguientes protecciones:

4.2.1.1. Antivirus de archivos residente (antispymware, antitroyano, antimalware, antiransomware, análisis de comportamiento y detección de anomalías, etc.) que verifique cualquier archivo creado, accedido o modificado;

4.2.1.2. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.

4.2.2. Capacidad de configurar el permiso de acceso a las funciones del antivirus con, como mínimo, opciones para las siguientes funciones:

4.2.2.1. Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);

4.2.2.2. Gerenciamiento de respaldo: Creación de copias de los objetos infectados en un reservorio de respaldo antes del intento de desinfectar o eliminar tal objeto, siendo de esta manera posible la recuperación de objetos que contengan informaciones importantes;

4.2.2.3. Gerenciamiento de cuarentena: Cuarentena de objetos sospechosos y corrompidos, guardando tales archivos en una carpeta de cuarentena;

4.2.2.4. Verificación por agendamiento: búsqueda de archivos infectados y sospechosos (incluyendo archivos dentro de un rango especificado); análisis de archivos; desinfección o eliminación de objetos infectados.

4.2.3. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otros software;

4.2.4. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;

4.2.5. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;

4.2.6. Capacidad de verificar objetos usando heurística;

4.2.7. Posibilidad de elegir la carpeta donde los archivos recuperados de respaldo y los archivos se grabarán

4.2.8. Posibilidad de elegir la carpeta donde se guardarán los respaldos y archivos en cuarentena

4.2.9. Debe contar con módulo de administración remoto a través de herramienta nativa o Webmin (herramienta nativa GNU-Linux).

## **5. Servidores Windows**

### **5.1. Compatibilidad:**

5.1.1. Windows Server 2019 todas las versiones

5.1.2. Windows Server 2016 todas las versiones

5.1.3. Windows Server 2012 todas las versiones

5.1.4. Windows Server 2008 todas las versiones, Service Pack 1 o superior

5.1.5. Windows Storage Server 2012 o superior

5.1.6. Hyper-V Server 2012 o superior

### **5.2. Características:**

5.2.1. Debe proporcionar las siguientes protecciones:

5.2.1.1. Antivirus de archivos residente (antispysware, antitroyano, antimalware, antiransomware, análisis de comportamiento y detección de anomalías, etc.) que verifique cualquier archivo creado, accedido o modificado;

5.2.1.2. Autoprotección contra ataques a los servicios/procesos del antivirus

5.2.1.3. Firewall con IDS

5.2.1.4. Control de vulnerabilidades de Windows y de los aplicativos instalados

5.2.2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota;

5.2.3. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora..

5.2.4. Capacidad de configurar el permiso de acceso a las funciones del antivirus con como mínimo, opciones para las siguientes funciones:

5.2.4.1. Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);

5.2.4.2. Gerenciamiento de tarea (crear o excluir tareas de verificación)

5.2.4.3. Lectura de configuraciones

5.2.4.4. Modificación de configuraciones

5.2.4.5. Gerenciamiento de respaldo y cuarentena

5.2.4.6. Visualización de informes

5.2.4.7. Gerenciamiento de informes

5.2.4.8. Gerenciamiento de claves de licencia

5.2.4.9. Gerenciamiento de permisos (agregar/excluir permisos superiores)

5.2.5. El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:

5.2.5.1. Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas;

5.2.5.2. Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados.

5.2.6. Capacidad de seleccionar por separado el número de procesos que ejecutarán funciones de barrido en tiempo real, el número de procesos que ejecutarán el barrido a demanda y el número máximo de procesos que pueden ser ejecutados en total.

5.2.7. Capacidad de reanudar automáticamente tareas de verificación que hayan sido interrumpidas por anomalías (corte de energía, errores, etc.)

5.2.8. Capacidad de automáticamente pausar y no iniciar tareas agendadas en caso de que el servidor esté funcionando con fuente ininterrumpida de energía (uninterruptiblePowersupply UPS)

5.2.9. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otros software;

5.2.10. Capacidad de configurar niveles de verificación diferentes para cada carpeta, grupo de carpetas o archivos del servidor.

5.2.11. Capacidad de bloquear acceso al servidor de máquinas infectadas y cuando una máquina intenta grabar un archivo infectado en el servidor.

5.2.12. Capacidad de crear una lista de máquinas que nunca serán bloqueadas aunque sean infectadas.

5.2.13. Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación;

5.2.14. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, (ej.: Win32.Trojan.banker) para que cualquier objeto detectado con el resultado elegido sea ignorado;

5.2.15. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;

5.2.16. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;

5.2.17. Capacidad de verificar solamente archivos nuevos y modificados;

5.2.18. Capacidad de elegir qué tipo de objeto compuesto será verificado (ej.: archivos comprimidos, archivos autodescompresores, .PST, archivos compactados por compactadores binarios, etc.)

5.2.19. Capacidad de verificar objetos usando heurística;

5.2.20. Capacidad de configurar diferentes acciones para diferentes tipos de amenazas;

5.2.21. Capacidad de agendar una pausa en la verificación;

5.2.22. Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo;

5.2.23. El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe:

5.2.23.1. Preguntar qué hacer, o;

5.2.23.2. Bloquear el acceso al objeto;

5.2.23.2.1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador);

5.2.23.2.2. Caso positivo de desinfección:

5.2.23.2.2.1. Recuperar el objeto para uso;

5.2.23.2.3. Caso negativo de desinfección:

5.2.23.2.3.1. Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador);

5.2.24. Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto.

5.2.25. Posibilidad de elegir la carpeta donde los archivos recuperados de respaldo y los archivos se grabarán

5.2.26. Posibilidad de elegir la carpeta donde se guardarán los respaldos y archivos en cuarentena

5.2.27. Debe contar con módulo que analice cada script ejecutado, buscando señales de actividad maliciosa.

## **6. Smartphones y tablets**

### **6.1. Compatibilidad:**

6.1.1. Apple iOS 10.0 o superior

6.1.2. Android OS 4.2 o superior

### **6.2. Características:**

6.2.1. Debe proporcionar las siguientes protecciones:

6.2.1.1. Protección en tiempo real del sistema de archivos del dispositivo — interceptación y verificación de:

6.2.1.1.1. Todos los objetos transmitidos usando conexiones wireless (puerta de infrarrojo, Bluetooth) y mensajes EMS, durante sincronismo con PC y al realizar descargas usando el browser.

6.2.1.1.2. Archivos abiertos en el smartphone

6.2.1.1.3. Programas instalados usando la interface del smartphone

6.2.1.2. Verificación de los objetos en la memoria interna del smartphone y en las tarjetas de expansión a pedido del usuario y de acuerdo con un agendamiento;

6.2.2. Deberá aislar en área de cuarentena los archivos infectados;

6.2.3. Deberá actualizar las bases de vacunas de modo agendado;

6.2.4. Deberá bloquear spam de SMS a través de Black lists (listas negras);

6.2.5. Deberá tener función de bloqueo del aparato en caso de que la SIM CARD sea cambiada por otra no autorizada;

6.2.6. Deberá tener función de limpieza de datos personales a distancia, en caso de robo, por ejemplo.

6.2.7. Deberá tener firewall personal;

6.2.8. Posibilidad de instalación remota utilizando Microsoft System Center Mobile Device Manager 2008 SP1

6.2.9. Posibilidad de instalación remota utilizando SybaseAfaria 6.5

6.2.10. Capacidad de detectar Jailbreak en dispositivos iOS

6.2.11. Capacidad de bloquear el acceso a sitios por categoría en dispositivos

6.2.12. Capacidad de bloquear el acceso a sitios phishing o maliciosos

6.2.13. Capacidad de crear contenedores de aplicativos, separando datos corporativos de datos personales

6.2.14. Capacidad de configurar white y blacklist (listas blancas y listas negras) de aplicativos.

## **7. Manejo de dispositivos móviles (MDM)**

### **7.1. Compatibilidad:**

7.1.1. Dispositivos conectados a través de Microsoft Exchange ActiveSync

7.1.1.1. Apple iOS

7.1.1.2. Android

7.1.2. Dispositivos con soporte a Apple Push Notification (APNs) service

7.1.2.1. Apple iOS 11.0 o superior

### **7.2. Características:**

7.2.1. Capacidad de aplicar políticas de ActiveSync a través del servidor Microsoft Exchange

7.2.2. Capacidad de ajustar las configuraciones de:

7.2.2.1. Sincronización de correo electrónico

7.2.2.2. Uso de aplicativos

7.2.2.3. Contraseña del usuario

7.2.2.4. Cifrado de datos

7.2.2.5. Conexión de medios extraíbles

- 7.2.3. Capacidad de instalar certificados digitales en dispositivos móviles
- 7.2.4. Capacidad de, en forma remota, resetear la contraseña de dispositivos iOS
- 7.2.5. Capacidad de, en forma remota, borrar todos los datos de dispositivos iOS
- 7.2.6. Capacidad de, en forma remota, bloquear un dispositivo iOS

## **8. Cifrado**

### **8.1. Características:**

- 8.1.1. El acceso al recurso cifrado (archivo, carpeta o disco) debe ser garantizado aún en caso de que el usuario haya olvidado la contraseña, a través de procedimientos de recuperación.
- 8.1.2. Utilizar, como mínimo, un algoritmo AES con clave de 256 bits.
- 8.1.3. Capacidad de cifrar completamente el disco duro de la máquina, agregando un ambiente de preboot para autenticación del usuario.
- 8.1.4. Capacidad de utilizar Single Sign-On para la autenticación de preboot.
- 8.1.5. Permitir crear varios usuarios de autenticación preboot.
- 8.1.6. Capacidad de crear un usuario de autenticación preboot común con una contraseña igual para todas las máquinas a partir de la consola de manejo.
- 8.1.7. Capacidad de cifrar drives extraíbles de acuerdo con una regla creada por el administrador, con las opciones:
  - 8.1.7.1. Cifrar solamente los archivos nuevos que sean copiados para el disco extraíble, sin modificar los archivos ya existentes.
  - 8.1.7.2. Cifrar todos los archivos individualmente.
  - 8.1.7.3. Cifrar el dispositivo entero, de manera que no sea posible listar los archivos y carpetas almacenadas.
  - 8.1.7.4. Cifrar el dispositivo en modo portátil, permitiendo acceder a los archivos en máquinas de terceros a través de una contraseña.
- 8.1.8. Capacidad de seleccionar carpetas y archivos (por tipo, o extensión) para ser cifradas automáticamente. En esta modalidad, los archivos deben estar accesibles para todas las máquinas gestionadas por la misma consola de manera transparente para los usuarios.
- 8.1.9. Capacidad de crear reglas de exclusiones para que ciertos archivos o carpetas nunca sean cifrados.
- 8.1.10. Capacidad de seleccionar aplicaciones que pueden o no tener acceso a los archivos cifrados.

## **9. Gerenciamiento de Sistemas:**

9.1. Capacidad de crear imágenes de sistema operativo remotamente y distribuir esas imágenes para computadoras gestionadas por la solución y para computadoras bare-metal.

9.2. Capacidad de detectar software de terceros vulnerables, creando así un informe de software vulnerables.

9.3. Capacidad de corregir las vulnerabilidades de software, haciendo el download centralizado de la corrección o actualización y aplicando esa corrección o actualización en las máquinas gestionadas de manera transparente para los usuarios.

9.4. Contar con tecnología de Control de Admisión de Red (NAC), con la posibilidad de crear reglas de qué tipos de dispositivos pueden tener accesos a recursos de la red.

9.5. Capacidad de gestionar licencias de software de terceros.

9.6. Capacidad de registrar cambios de hardware en las máquinas gestionadas.

9.7. Capacidad de gestionar un inventario de hardware, con la posibilidad de registro de dispositivos (ej.: router, switch, proyector, accesorio, etc.), informando fecha de compra, lugar donde se encuentra, servicetag, número de identificación y otros.

## **10. Servidores de correo electrónico Windows Exchange:**

10.1. Características:

10.1.1. Debe utilizar las tecnologías VSAPI 2.0, 2.5 y 2.6;

10.1.2. Capacidad de iniciar varias copias del proceso de antivirus;

10.1.3. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.

10.1.4. Capacidad de verificar carpetas públicas, correos electrónicos enviados, recibidos y almacenados contra virus, spywares, adwares, gusanos, troyanos y riskwares;

10.1.5. Capacidad de verificar carpetas públicas y correos electrónicos almacenados de forma agendada, utilizando las últimas vacunas y heurística;

10.1.6. El antivirus, al encontrar un objeto infectado, debe:

10.1.6.1. Desinfectar el objeto, notificando el remitente, destinatario y administradores, o

10.1.6.2. Excluir el objeto, sustituyéndolo por una notificación;

10.1.6.3. Bloquear el acceso al objeto;

10.1.6.3.1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador);

10.1.6.3.2. Caso positivo de desinfección:

10.1.6.3.2.1. Recuperar el objeto para uso;

10.1.6.3.3. Caso negativo de desinfección:

10.1.6.3.3.1. Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador);

10.1.7. Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto.

10.1.8. Capacidad de enviar notificaciones sobre virus detectados para el administrador, para el destinatario y remitente del mensaje infectado.

10.1.9. Capacidad de grabar logs de actividad de virus en los eventos del sistema y en los logs internos de la aplicación;

10.1.10. Capacidad de detectar diseminación en masa de correos infectados, informando al administrador y registrando tales eventos en los logs del sistema y de la aplicación.

## **11. Funcionalidades de Detección y Respuesta de Endpoints**

11.1. La solución debe operar mediante una única consola tanto en entorno local como en la nube.

11.2. La solución debe incluir módulos EDR

11.3. La solución debe contar con funciones de automatización que garanticen la solución rápida de incidentes.

11.4. Capacidad de visualización de alertas de seguridad de los endpoints.

11.5. Capacidad de configurar respuestas automatizadas para amenazas descubiertas en todos los endpoints basadas en exploraciones de indicadores de compromiso - IoC.

11.6. Capacidad de respuesta instantánea a incidentes tras el descubrimiento

11.7. Las opciones de respuesta deben incluir:

11.7.1. aislar el host

11.7.2. poner en cuarentena el archivo

11.7.3. iniciar el análisis del host

11.7.4. impedir que se ejecute el archivo.

11.8. Capacidad de brindar información acerca de:

11.8.1. Alcance de la amenaza.

11.8.2. Estado de la amenaza: activo y desactivado.

11.8.3. Identificación de los hosts y cuentas de usuarios afectados.

11.8.4. Origen de la amenaza.

11.9. Capacidad de neutralizar amenazas mediante respuesta automática.

11.10. Capacidad de reacción inmediata a los incidentes detectados.

## 12. Servidor Sandbox

12.1. La propuesta debe incluir la instalación de un servidor ON-PREMISE Sandbox que se integre a la suíte de seguridad instalada en los endpoints y automatice los procesos de detección de archivos sospechosos.

12.2. La solución debe permitir realizar un análisis dinámico y detallado de las ciberamenazas desconocidas, dirigidas y evasivas

## 13. Protección para entornos Híbridos para escritorios virtuales

13.1. La herramienta debe incluir una solución libre de agente que se integre a los hipervisores de VMWare.

13.2. La herramienta debe incluir una solución con agente liviano para hipervisores Hyper-V y Citrix

## 14. Términos a tener en cuenta:

14.1. El proveedor deberá incluir con la propuesta un curso de Ciberseguridad, con una carga horaria de 12 horas como mínimo para tres personas, incluyendo los siguientes puntos.

14.1.1. Seguridad en entornos Windows y GNU/Linux.

14.1.2. Estrategias de Defensa.

14.1.3. Definición de políticas de Seguridad en la Institución.

14.2. Contar como mínimo con 3 profesionales certificados como Kaspersky KL Certified Professional o superior.

14.3. Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar **planilla de IPS y/o certificados de inscripción en IPS.**

14.4. Contar con 10 contratos o facturas de la provisión del Software ofertado entre los años 2018, 2019 y 2020.

14.5. Implementación de todos los módulos de la herramienta en todo el parque de equipos.

14.6. Capacitación de la herramienta a todas las personas involucradas en el departamento de tecnología y de seguridad de la información.

14.7. Soporte técnico prioritario 24x7 con tiempo de respuesta inferior a 3 horas para Asunción y 24 horas para el interior del país incluido durante todo el periodo de licenciamiento.

14.8. Cantidad de tickets de soporte ilimitados.

## Identificación de la unidad solicitante y justificaciones

- **Identificar el nombre, cargo y la dependencia de la Institución de quien solicita el llamado a ser publicado:** DIEGO POPOFF, Encargado de la Gerencia Departamental de Infraestructura de la Gerencia de Área de TI
- **Justificar la necesidad que se pretende satisfacer mediante la contratación a ser realizada:** El Banco Nacional de Fomento, tiene la imperiosa necesidad de disponer de un software de antivirus, a fin de disponer de una herramienta que cubra la posibilidad de ser afectado por cualquier tipo de virus. Es importante mencionar, la importancia del mismo, pues minimiza en gran manera, el riesgo de ser atacado por virus, que traerá consecuencias desastrosas para nuestra institución.
- **Justificar la planificación. (si se trata de un llamado periódico o sucesivo, o si el mismo responde a una necesidad temporal):** Como este llamado tienen una duración de 36 (treinta y seis) meses, una vez que concluya este contrato, el banco, dispondrá de un nuevo llamado, a fin de tener actualizado esta herramienta tan necesaria para la entidad.
- **Justificar las especificaciones técnicas establecidas:** Las EETT establecidas, para el presente llamado, son las especificaciones que consideramos necesarias, pues se ajustan a las necesidades de nuestro banco, en materia de antivirus

## Plan de entrega de los bienes

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

Ítem	Descripción del bien	Cantidad	Unidad de medida de los bienes	Lugar donde los bienes serán entregados	Fecha(s) final(es) de los bienes
1	Adquisición de Licencias Software Soporte Técnico Antivirus, 2000 unidades	2000	Unidad	Gerencia de Área de Tecnología Informática del Banco Nacional de Fomento, en Casa Matriz	Una vez suscrito el Contrato (diez) días corridos.

---

### **Plan de entrega de los servicios**

No Aplica.

---

### **Planos y diseños**

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

No Aplica

---

### **Embalajes y documentos**

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

No Aplica

---

### **Inspecciones y pruebas**

Las inspecciones y pruebas serán como se indican a continuación:

No Aplica

---

### **Indicadores de Cumplimiento**

El documento requerido para acreditar el cumplimiento contractual será:

Planificación de indicadores de cumplimiento:

Será presentado 1 (un) Informe.

Frecuencia: única vez

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA (se indica la fecha que debe presentar según el PBC)
Nota de Remisión / Acta de recepción 1	Nota de Remisión / Acta de recepción	

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.

## Criterios de Adjudicación

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 procesos de contratación en los cuales se aplique la modalidad de contrato abierto, se efectuará por las cantidades o montos máximos solicitados en el llamado, sin que ello implique obligación de la convocante de requerir la provisión de esa cantidad o monto durante 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 requerida, 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 llamados en los cuales se aplique la modalidad 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

La comunicación de la adjudicación a los oferentes será como sigue:

1. Dentro de los cinco (5) días corridos de haberse resuelto la adjudicación, la convocante comunicará a través del Sistema de Información de Contrataciones Públicas, copia del informe de evaluación y del acto administrativo de adjudicación, los cuales serán puestos a disposición pública en el referido sistema. Adicionalmente el sistema generará una notificación a los oferentes por los medios remotos de comunicación electrónica pertinentes, la cual será reglamentada por la DNCP.
2. En sustitución de la notificación a través del Sistema de Información de Contrataciones Públicas, las convocantes podrán dar a conocer la adjudicación por cédula de notificación a cada uno de los oferentes, acompañados de la copia íntegra del acto administrativo y del informe de evaluación. 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.

La misma deberá ser solicitada dentro de los dos (2) días hábiles siguientes en que el oferente haya tomado conocimiento de los términos del Informe de Evaluación de Ofertas.

La convocante deberá dar respuesta a dicha solicitud dentro de los dos (2) días hábiles de haberla recibido y realizar la audiencia en un plazo que no exceda de dos (2) días hábiles siguientes a la fecha de respuesta al oferente.

---

## 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
a) Certificado de no encontrarse en quiebra o en convocatoria de acreedores expedido por la Dirección General de Registros Públicos;
b) Certificado de no hallarse en interdicción judicial expedido por la Dirección General de Registros Públicos;
c) Constancia de no adeudar aporte obrero patronal expedida por el Instituto de Previsión Social;
d) 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;
e) 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.
f) Certificado de Cumplimiento Tributario vigente a la firma del contrato.
2. Documentos. Consorcios
a) Cada integrante del consorcio que sea una persona física o jurídica deberá presentar los documentos requeridos para oferentes individuales especificados en los apartados precedentes.
b) Original o fotocopia del consorcio constituido.
c) Documentos que acrediten las facultades del firmante del contrato para comprometer solidariamente al consorcio.
d) 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.

# CONDICIONES CONTRACTUALES

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

## Interpretación

### 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.

## 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 seguirá 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 resultara 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 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.

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 participen 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 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 Información del Personal (FIP) y en el Formulario de Informe de Servicios Personales (FIS), a través del SIPE.

2. Cuando ocurra algún cambio en la nómina del personal o de los subcontratistas propuestos, el proveedor o contratista está obligado a actualizar el FIP.

3. Como requerimiento para efectuar los pagos a los proveedores o contratistas, la contratante, a través del procedimiento establecido para el efecto por la entidad previsional, verificará que el proveedor o contratista se encuentre al día en el cumplimiento con sus obligaciones para con el Instituto de Previsión Social (IPS).

4. La contratante podrá realizar las diligencias que considere necesarias para verificar que la totalidad de las personas que prestan servicios personales en relación de dependencia para la contratista y eventuales subcontratistas se encuentren debidamente individualizados en los listados recibidos.

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

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

---

## **Formas y condiciones de pago**

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

1. Documentos Genéricos:

- a. Nota de remisión u orden de prestación de servicios según el objeto de la contratación;
- b. La factura de pago, con timbrado vigente, la cual deberán expresar claramente por separado el Impuesto al Valor Agregado (IVA) de conformidad con las disposiciones tributarias aplicables. En ningún caso el valor total facturado podrá exceder el valor adjudicado o las adendas aprobadas;
- c. REPSE (registro de prestadores de servicios) todos los que son prestadores de servicios;
- d. Certificado de Cumplimiento Tributario;
- e. Constancia de Cumplimiento con la Seguridad Social;
- f. Formulario de Informe de Servicios Personales (FIS).

Otras formas y condiciones de pago al proveedor en virtud del contrato serán las siguientes: Se realizará en un sólo pago. Los proveedores adjudicados deberán habilitar una cuenta en el Banco Nacional de Fomento, a fin de realizar la acreditación del pago correspondiente y así agilizar el proceso de liquidación de cancelación de obligaciones del Banco, para el efecto serán exonerados los requisitos de mantenimiento de Cajas de Ahorros, consistente en el depósito inicial y saldo promedio mínimo requerido; además deberán presentar documentos requeridos por la SEPRELAD según el Artículo 33 de la Resolución 70/2019 política de Conozca a su proveedor formulario Anexo 2 Perfil del cliente. Así mismo, se deberá adjuntar al legajo documentario copia de la nota de notificación de adjudicación emitida por la Gerencia Departamental Operativa de Contrataciones

- 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 de 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 calendario 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.

## **Solicitud de Pago de Anticipo**

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

No Aplica

## Reajuste

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

El precio del contrato estará sujeto a reajustes. EL **PROVEEDOR** solicitará por escrito a La **contratante** el reajuste de precios exponiendo la causa del mismo.

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

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

V1= Reajuste de la Oferta

P= Precio de los Bienes (en la Oferta)

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

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

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

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

## Porcentaje de multas

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

0,50 %

La contratante podrá deducir en concepto de multas una suma equivalente al porcentaje del precio de entrega de los bienes atrasados, por cada día de atraso indicado en este apartado. La contratante podrá rescindir administrativamente el contrato cuando el valor de las multas supere el monto de la Garantía de Cumplimiento de Contrato.

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:

0,10

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.

## **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° 63 de la Ley N° 2051/2003.

1. Cuando el sistema de adjudicación adoptado sea de abastecimiento simultáneo las ampliaciones de los contratos se registrarán por las disposiciones contenidas en la Ley N° 2051/2003, sus modificaciones y reglamentaciones, que para el efecto emita la DNCP.
2. Tratándose de contratos abiertos, las modificaciones a ser introducidas se registrarán atendiendo a la reglamentación vigente.
3. La celebración de un convenio modificador conforme a las reglas establecidas en el artículo N° 63 de la Ley 2051/2003, que constituyan condiciones de agravación del riesgo cuando la Garantía de Cumplimiento de Contrato sea formalizada a través de póliza de caución, 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.

## **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.
6. 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;
- ii. Si el proveedor no cumple con cualquier otra obligación en virtud del contrato;
- 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 Fiel 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; o
- vi. En los demás casos previstos en este apartado.

## 2. Terminación por insolvencia o quiebra

La contratante podrá rescindir 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:

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

## Otras causales de terminación del contrato

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

No Aplica

## Resolución de Conflictos a través del Arbitraje

Las partes se someterán a Arbitraje:

No

En caso que la convocante adopte el arbitraje como mecanismo de resolución de conflicto, la cláusula arbitral que registrará a las partes es la siguiente:

"Todas las controversias que deriven del presente contrato o que guarden relación con éste serán resueltas definitivamente por arbitraje, conforme con las disposiciones de la Ley N° 2051/03 "De Contrataciones Públicas", de la Ley N° 1879/02 "De arbitraje y

mediación" y las condiciones del Contrato. El procedimiento arbitral se llevará a cabo ante el Centro de Arbitraje y Mediación del Paraguay (en adelante, "CAMP"). El tribunal estará conformado por tres árbitros designados de la lista del cuerpo arbitral del CAMP, que decidirá conforme a derecho, siendo el laudo definitivo y vinculante para las partes. Se aplicará el reglamento respectivo y demás disposiciones que regule dicho procedimiento al momento de ser requerido, declarando las partes conocer y aceptar los vigentes, incluso en orden a su régimen de gastos y costas, considerándolos parte integrante del presente contrato. Para la ejecución del laudo arbitral, o para dirimir cuestiones que no sean arbitrables, las partes se someterán a la jurisdicción de los tribunales de la ciudad de Asunción, República del Paraguay".

---

## 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 penal 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 (Declaratoria de Integridad).

# 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.

