

**PLIEGO DE BASES Y CONDICIONES**

---

Convocante:

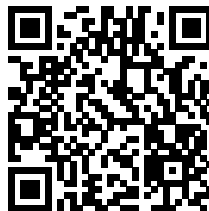
**Ministerio de Economía y Finanzas**  
**Uoc Ministerio de Economía y Finanzas**

Nombre de la Licitación:

**ADQUISICIÓN DE EQUIPAMIENTO PARA EL  
DATACENTER DE LA DGAF (MEF)**  
(versión 1)

ID de Licitación:

**446703**



Modalidad:

**Licitación Pública Nacional**

Publicado el:

**02/10/2024**

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

# RESUMEN DEL LLAMADO

## Datos de la Convocatoria

ID de Licitación:	446703	Nombre de la Licitación:	ADQUISICIÓN DE EQUIPAMIENTO PARA EL DATACENTER DE LA DGAF (MEF)
Convocante:	Ministerio de Economía y Finanzas	Categoría:	43000000 - Tecnologías de Información, Telecomunicaciones y Radiodifusiones
Unidad de Contratación:	Uoc Ministerio de Economía y Finanzas	Tipo de Procedimiento:	LPN - Licitación Pública Nacional

## Etapas y Plazos

Lugar para Realizar Consultas:	A TRAVÉS DEL SICP	Fecha Límite de Consultas:	10/10/2024 12:00
Lugar de Entrega de Ofertas:	Ministerio de Economía y Finanzas - CUOC - Estrella 345 c/Chile - Edificio Citicentro 5° Piso	Fecha de Entrega de Ofertas:	17/10/2024 08:15
Lugar de Apertura de Ofertas:	Ministerio de Economía y Finanzas - CUOC - Estrella 345 c/Chile - Edificio Citicentro 5° Piso	Fecha de Apertura de Ofertas:	17/10/2024 08:30

## Adjudicación y Contrato

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

## Datos del Contacto

Nombre:	Andrés María Soria Martínez	Cargo:	COORDINADOR UOC
Teléfono:	021 4146028	Correo Electrónico:	uoc@hacienda.gov.py

# DATOS DE LA CONVOCATORIA

Los Datos de la Licitación constituye la información proporcionada por la convocante para establecer las condiciones a considerar del proceso particular, y que sirvan de base para la elaboración de las ofertas por parte de los potenciales oferentes.

## Datos de la Convocatoria

Los datos de la licitación serán consignados en esta sección y en el Sistema de Información de Contrataciones Públicas (SICP), los mismos forman parte de los documentos del presente procedimiento de contratación.

## Difusión de los documentos de la Convocatoria

Todos los datos y documentos de este procedimiento de contratación deben ser obtenidos directamente del (SICP). Es responsabilidad del oferente examinar todos los documentos y la información de la convocatoria que obren en el mismo.

## Contratación Pública Sostenibles - CPS

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

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

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

## Aclaración de los documentos de la convocatoria

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

Se prorrogará de forma automática en el SICP, el plazo tope para la realización de consultas cuando la fecha del acto de

presentación de ofertas sea modificada.

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

La convocante podrá optar por responder las consultas en la Junta de Aclaraciones o podrá diferirlas, para que sean respondidas conforme con los plazos de respuestas o emisión de adendas. En todos los casos se deberá levantar acta circunstanciada.

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

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

## Formato y firma de la oferta

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

## Plazo para presentar las ofertas

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

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

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

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

## Oferentes en consorcio

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

Para ello deberán presentar una escritura pública de constitución que reúna las características previstas en el Decreto reglamentario o un acuerdo de intención de participación en contrato de consorcio, el cual se deberá formalizar por escritura pública en caso de resultar adjudicados, antes de la firma del contrato.

Los integrantes de un consorcio no podrán presentar ofertas individuales ni conformar más de un consorcio en un mismo lote

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

En todo lo demás deberán ajustarse a lo dispuesto en la normativa legal vigente.

## Idioma de la oferta

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

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

No Aplica

## Precio y formulario de la oferta

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

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

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

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

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

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

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

4. El precio del contrato que cobre el proveedor por los bienes y/o servicios suministrados en virtud del contrato no podrá ser diferente a los precios unitarios cotizados en su oferta, excepto por cualquier ajuste previsto en el mismo.
5. En caso que se requiera el desglose de los componentes de los precios será con el propósito de facilitar a la convocante la comparación de las ofertas.
6. En las contrataciones internacionales los oferentes no domiciliados en el territorio de la República deberán manifestar en su oferta que los precios que presentan en su propuesta económica no se cotizan en condiciones de prácticas desleales de comercio internacional en su modalidad de discriminación de precios o subsidios.

---

## **Abastecimiento simultáneo**

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

No Aplica

---

## **Moneda de la oferta y pago**

La moneda de la oferta y pago será:

Guaraníes

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

---

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

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

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

Cantidad de copias requeridas:

0 copias

---

## **Método de presentación de ofertas**

El método de presentación de ofertas para esta convocatoria será:

Un sobre

En caso de presentación física, los sobres deberán:

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

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

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

## Documentos de la oferta

El pliego, sus adendas y aclaraciones no forman parte de la oferta, por lo que no se exigirá la presentación de copias de los mismos con la oferta.

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

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

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

## Ofertas Alternativas

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

No Aplica

## Periodo de validez de las ofertas

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

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

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

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

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

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

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

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



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

## **Retiro, sustitución y modificación de las ofertas**

1. Un oferente podrá retirar, sustituir o modificar su oferta después de presentada mediante el envío de una comunicación por escrito, debidamente firmada por el representante autorizado. La sustitución o modificación correspondiente de la oferta deberá acompañar dicha comunicación por escrito.

2. Todas las comunicaciones deberán ser:

- a) Presentadas conforme a la forma de presentación e identificación de las ofertas y además los respectivos sobres deberán estar marcados "RETIRO", "SUSTITUCION" o "MODIFICACION";
- b) Recibidas por la convocante antes del plazo límite establecido para la presentación de las ofertas;

Las ofertas cuyo retiro, sustitución o modificación fuere solicitada serán devueltas sin abrir a los oferentes remitentes, durante el acto de apertura de ofertas.

3. Ninguna oferta podrá ser retirada, sustituida o modificada durante el intervalo comprendido entre la fecha límite para presentar ofertas y la expiración del período de validez de las ofertas indicado en el Formulario de Oferta o cualquier extensión si la hubiere, caso contrario, se hará efectiva la Garantía de Mantenimiento de Oferta.

Cuando la presentación de oferta se realice a través del módulo de oferta electrónica la misma deberá sujetarse a la reglamentación vigente

## **Apertura de ofertas**

1. La entidad convocante procederá a la apertura de las ofertas y, en caso de existir notificaciones de retiro, sustitución o modificación de las propuestas, se leerá durante el acto público en presencia de los oferentes o sus representantes según la hora, fecha y lugar previamente establecidos en el SICP.

2. Cuando la presentación de la oferta sea electrónica, el acto de apertura deberá sujetarse a la reglamentación vigente, en la hora y fecha establecida en el SICP.

3. Primero se procederá a verificar los sobres de las ofertas recibidas, marcados como:

- a) "RETIRO": Se leerán en voz alta y el sobre con la oferta correspondiente no será abierto sino devuelto al oferente remitente. No se permitirá el retiro de ninguna oferta a menos que la comunicación de retiro contenga una autorización válida y sea leída en voz alta en el acto de apertura de las ofertas.
- b) "SUSTITUCION": Se leerán en voz alta y se intercambiará con la oferta correspondiente que está siendo sustituida; la oferta sustituida no se abrirá y se devolverá al oferente remitente. No se permitirá la sustitución de ninguna oferta a menos que la comunicación de sustitución contenga una autorización válida y sea leída en voz alta en el acto de apertura de las ofertas.
- c) "MODIFICACION": Se abrirán y leerán en voz alta con la oferta correspondiente. No se permitirá ninguna modificación a las ofertas a menos que la comunicación de modificación contenga una autorización válida y sea leída en voz alta en el acto de apertura de las ofertas. Solamente se considerarán en la evaluación los sobres que se abren y leen en voz alta durante el Acto de Apertura de las Ofertas.

4. Los representantes de los oferentes que participen en la apertura de las ofertas deberán contar con autorización suficiente para suscribir el acta y para revisar los documentos de los demás oferentes, bastando para ello la presentación de una

autorización escrita del firmante de la oferta, esta autorización podrá ser incluida en el sobre oferta o ser portada por el representante.

5. Se solicitará a los representantes de los oferentes presentes que firmen el acta. La omisión de la firma por parte de un oferente no invalida el contenido y efecto del acta. Se distribuirá una copia del acta a todos los presentes.

6. Las ofertas sustituidas y modificadas, que no sean abiertas y leídas en voz alta durante el acto de apertura no podrán ser consideradas para la evaluación sin importar las circunstancias y serán devueltas sin abrir a los remitentes.

7. La falta de firma en un documento sustancial, es considerada una omisión sustancial que no podrá ser subsanada en ninguna oportunidad una vez abiertas las ofertas. En cuanto a la garantía de mantenimiento de oferta deberá estar debidamente extendida.

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

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

---

## Visita al sitio de ejecución del contrato

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

No Aplica

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

Cuando la convocante haya establecido que será requisito de participación, el oferente que conozca el sitio podrá declarar bajo fe de juramento conocer el sitio y que cuenta con la información suficiente para preparar la oferta y ejecutar el contrato.

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

Las condiciones de participación no deberán ser restrictivas ni limitativas.

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

Los representantes de los oferentes que asistan podrán contar con una autorización, bastando para ello la presentación de una nota del oferente. **La falta de presentación de esta autorización no impide su participación en la visita o inspección técnica.**

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

---

## Incoterms

La edición de incoterms para esta licitación será:

No Aplica

Las expresiones DDP, CIP, FCA, CPT y otros términos afines, se regirán por las normas prescriptas en la edición vigente de los Incoterms

publicada por la Cámara de Comercio Internacional.

Durante la ejecución contractual, el significado de cualquier término comercial, así como los derechos y obligaciones de las partes serán los prescritos en los Incoterms, a menos que sea inconsistente con alguna disposición del Contrato.

---

## Autorización del Fabricante

Los ítems a los cuales se le requerirá Autorización del Fabricante son los indicados a continuación:

Todos los bienes deberán contar con autorización del fabricante de acuerdo a lo estipulado en las Especificaciones Técnicas.

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

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

---

## Muestras

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

No Aplica

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

---

## Tiempo de funcionamiento de los bienes

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

36 meses

---

## Plazo de reposición de bienes

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

48 horas

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

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

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

2. Si el proveedor después de haber sido notificado, no cumple dentro del plazo establecido, la contratante, procederá a tomar medidas necesarias para remediar la situación, por cuenta y riesgo del proveedor y sin perjuicio de otros derechos que la contratante pueda ejercer contra el proveedor en virtud del contrato.

---

## **Periodo de validez de la Garantía de los bienes**

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

36 meses

---

## **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.

# REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN

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

## Condición de Participación

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

Los oferentes domiciliados en la República del Paraguay, que pretendan participar en un procedimiento de contratación, no deberán estar comprendidos en las prohibiciones o limitaciones para presentar propuestas y contratar con el Estado, establecidas en la Ley N° 7021/22 "DE SUMINISTROS Y CONTRATACIONES PUBLICAS".

## Sucursales

En los casos de procedimientos de contratación de carácter nacional podrán participar las sucursales de las matrices internacionales constituidas en la República del Paraguay. Solo serán admitidas como criterios de adjudicación las capacidades, experiencia y aptitudes de la sucursal recabadas desde su constitución, sin admitirse la utilización de las cualidades de la casa matriz u otras filiales o sucursales.

## Requisitos de Calificación

**Calificación Legal.** Los oferentes deberán declarar que no se encuentran comprendidos en las limitaciones o prohibiciones para contratar con el Estado, según lo establecido en el artículo 21 de la Ley N° 7021/22 en concordancia con el Artículo 19 de su Decreto Reglamentario. Esta declaración forma parte del formulario de oferta en los casos que el procedimiento de contratación sea convencional y formulario de Oferta electrónica en el caso que se utilice el módulo de oferta electrónica.

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

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

1. Verificará que el oferente haya proporcionado el formulario de ofertas, la declaración jurada de no estar comprendido en las prohibiciones y limitaciones para presentar propuesta y contratar, y además las constancias de registro de estructura jurídica y de beneficiarios finales.
2. Verificará los registros del personal de la convocante para detectar si el oferente o sus representantes, se hallan comprendidos en el artículo 21 de la Ley N° 7021/22.
3. Verificará por los medios disponibles, si el oferente y los demás sujetos individualizados en las prohibiciones o limitaciones contenidas en los incisos, aparecen en la base de datos del SINARH del VICE MINISTERIO DE CAPITAL

#### HUMANO Y GESTION ORGANIZACIONAL.

4. Si se constatará que alguno de las personas mencionadas en el párrafo anterior figura en la base de datos del SINARH del VICE MINISTERIO DE CAPITAL HUMANO Y GESTION ORGANIZACIONAL, el comité analizará acabadamente si tal situación le impedirá ejecutar el contrato, exponiendo los motivos para aceptar o rechazar la oferta, según sea el caso.
5. Verificará que el oferente haya proporcionado el formulario de Declaración de Personas, debidamente firmado, conforme a los estándares establecidos, y cotejará los datos con las personas físicas inhabilitadas que constan en el registro de “Sanciones a Proveedores” del SICP. Con el objeto de verificar si los directores, gerentes, socios gerentes, quienes ejerzan la administración, accionistas, cuotapartistas o propietarios se encuentren dentro de los criterios contemplados en los incisos g), h), i), y j) de la Ley 7021/22.
6. El comité podrá recurrir a fuentes públicas o privadas de información, para verificar los datos proporcionados por el oferente y las obrantes en el registro de inhabilitados de la DNCP.
7. Si el Comité confirma que el oferente o sus integrantes poseen impedimentos en virtud a lo dispuesto en el artículo 21 de la Ley N° 7021/22, la oferta será rechazada y se remitirán los antecedentes a la DNCP para los fines pertinentes.

## Metodo de Evaluación

Basado únicamente en precio

## Análisis de precios ofertados

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

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

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

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

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

## Composición de Precios

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

ÍTEM	DESCRIPCIÓN	MONTO
1	COSTO DEL PRODUCTO	
2	IMPUESTO	
3	GASTOS OPERACIONALES	
4	GASTOS ADMINISTRATIVOS	
5	UTILIDAD	
6	PRECIO TOTAL	

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

## Margen de preferencia en procedimientos de contratación de carácter internacional

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

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

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

## Requisitos documentales para evaluación de las condiciones de participación.

### 1. Formulario de Oferta (\*)

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

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

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

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

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

#### **8.1. Personas Físicas.**

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

#### **8.2. Personas Jurídicas.**

1. Fotocopia simple de los documentos que acrediten la existencia legal de la persona jurídica tales como la Escritura Pública de Constitución y protocolización de los Estatutos Sociales. Los estatutos deberán estar inscriptos en la Sección Personas Jurídicas de la Dirección de Registros Públicos. (\*)
2. Constancia de inscripción en el Registro Único de Contribuyentes. (\*)
3. Fotocopia simple de los documentos de identidad de los representantes o apoderados de la sociedad. (\*)
- d. Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al oferente. Estos documentos pueden consistir en: un poder suficiente otorgado por Escritura Pública (no es necesario que esté inscripto en el Registro de Poderes); o los documentos societarios que justifiquen la representación del firmante, tales como las actas de asamblea y de directorio en el caso de las sociedades anónimas. (\*)

#### **8.3. Oferentes en Consorcio.**

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



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

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

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

## Capacidad Financiera

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

1. **CONTRIBUYENTES DE IRACIS:** Deberán cumplir los siguientes parámetros:

Ratio de Liquidez: activo corriente/ pasivo corriente. Deberá ser igual o mayor que 1 en promedio en los años 2021, 2022 y 2023.

Endeudamiento: pasivo total/activo total. No deberá ser mayor a 0,80 en promedio, en los años 2021, 2022 y 2023.

Rentabilidad: Porcentaje de utilidad después de impuestos o perdida con respecto al Capital. El promedio en los años 2021, 2022 y 2023. no deberá ser negativo.

2. **CONTRIBUYENTES DE IRPC:** Deberán cumplir el siguiente parámetro:

Eficiencia: Ingreso/Egreso. Deberá ser igual o mayor que 1, el promedio en los años 2021, 2022 y 2023.

3. **CONTRIBUYENTES DE IRP:** Deberán cumplir el siguiente parámetro:

Eficiencia: Ingreso/Egreso. Deberá ser igual o mayor que 1, el promedio en los años 2021, 2022 y 2023.

**OBSERVACIÓN:**

En el caso de consorcios, se sumarán los promedios y los coeficientes, respectivamente, de cada miembro, a los efectos de promediar los resultados.

## Requisitos documentales para la evaluación de la capacidad financiera

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

a	Balance General y Cuadro de Resultados de los años 2021, 2022 y 2023, para contribuyentes de IRACIS o su equivalente según el nuevo Régimen Tributario.
b	Formulario de los años 2021, 2022 y 2023, para contribuyentes de IRPC o su equivalente según el nuevo Régimen Tributario.
c	Formulario de los años 2021, 2022 y 2023, para contribuyentes de IRP o su equivalente según el nuevo Régimen Tributario.

---

## Experiencia requerida

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

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

Demostrar la experiencia en Provisión de equipos informáticos con facturaciones de venta y/o recepciones finales por un monto equivalente al 50 % como mínimo del monto total ofertado en la presente licitación, de los: últimos 3 años.

- La empresa deberá tener una antigüedad mínima en el mercado, de por lo menos 5 (cinco) años, contados desde la inscripción en el Registro Único del Contribuyente.
- Demostrar la experiencia en **Provisión de equipos informáticos** con copias de contratos ejecutados, facturaciones de venta y/o recepciones finales por un monto equivalente al 50% como mínimo del monto total ofertado en la presente licitación, se tendrá en cuenta el promedio de los últimos 3 (tres) años (2021, 2022 y/o 2023) para el cumplimiento de este requisito.

---

## Requisitos documentales para la evaluación de la experiencia

1. *Copia de facturas o remitos o contratos o recepciones finales u otra documentación que acredite las provisiones realizadas en los últimos tres años.*

2. *Constancia de Inscripción en el Registro Único del Contribuyente.*

---

## Capacidad Técnica

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

1. Declaración Jurada de contar con la Capacidad de brindar soporte técnico local en la República del Paraguay durante el periodo de garantía.
2. Considerando que el presente llamado se trata de provisión de equipos y servicios conexos, se requiere que el Oferente/Proveedor cuente con una estructura de trabajo estandarizada/normalizada, trazable y auto gestionada que permita el cumplimiento efectivo de la provisión, transporte e instalación, por tanto se necesita que posea certificación ISO 9001/2015 con alcance de Servicio de Soporte, especializados para el Sector Gobierno o similar; La similitud debe basarse en los mismos criterios que solicita o certifica la Norma ISO 9001/2015 con respecto a la Calidad de la gestión de procedimientos de provisión de bienes y/o servicios.
3. Declaración jurada en donde indique que dará cumplimiento a las garantías requeridas por el periodo de 36 meses.
4. Nota en la que liste nombre apellido y número de cedula de los técnicos certificados en las marcas mencionadas para cubrir los servicios contratados, adjuntar currículum y copia del certificado.
5. DD.JJ. que el personal asignado por la empresa Contratada se ceñirá a las normas y procedimientos de seguridad del Ministerio de Economía y Finanzas.
6. Declaración Jurada en que la Empresa se compromete a cumplir con todos los puntos solicitados en las Especificaciones

Técnicas del PBC.

7. Los técnicos deberán estar en la planilla de IPS. Comprobada con constancia emitida por el IPS (Instituto de Previsión Social).
8. El Oferente debe demostrar experiencia en la provisión e instalación de Routers/Firewalls durante el periodo 2020 - 2023 demostrado de la siguiente manera: Copias de Facturaciones y/o contratos de haber proveído a Entidades Públicas y/o Privadas por lo menos el 50% (cincuenta por ciento) del monto de la oferta presentada.

#### **Para el Lote 1:**

El oferente deberá contar con al menos:

- 01 (uno) profesional con certificado vigente de PMP (Project Management Professional) certificado por el PMI (Project Manager Institute) o certificación vigente Scrum Master con reconocimiento internacional o certificaciones equivalentes, para la planificación, ejecución y control de los trabajos, Los cuales deberán ser verificable con la planilla de IPS y/o Estatuto de la empresa.
- 02 (dos) técnicos certificados por el fabricante de los equipos ofertados. La experiencia del personal en la solución ofertada deberá ser demostrable con la presentación del Certificado de Especialista emitido por el fabricante, demostrable con la planilla de IPS.
- 02 (dos) técnicos certificados en el producto de virtualización de Huawei Virtualization Suite Platinum Edition los cuales deben ser verificable con el formulario de inscripción y la última planilla de IPS.
- 02 (dos) técnicos certificados en Storage Huawei de nivel profesional con certificado vigente y verificable. La experiencia del personal debe ser demostrable con la presentación del Certificado de Especialista en Storage Huawei, el personal propuesto debera ser demostrable con la planilla de IPS y/o Estatuto de la empresa.
- 02 (dos) técnicos certificados en Veritas Backup Exec. la experiencia del personal deberá ser demostrable con la presentación del Certificado de Especialista en Veritas Backup, el personal propuesto deberá ser demostrable con la planilla de IPS y/o Estatuto de la empresa.

#### **Para el Lote 2:**

- El oferente deberá contar con al menos 2(dos) técnicos certificados en la marca ofertada, los mismos deberán estar inscriptos en IPS. Se deberá presentar última planilla vigente del Aporte Obrero Patronal IPS para garantizar que el personal propuesto pertenece a la nómina de funcionarios permanentes de la empresa. Además, será un requisito indispensable que la empresa oferente esté autorizada por el Fabricante a prestar el servicio técnico y el cambio de partes por garantía. Es también aceptable para la Convocante que el oferente esté debidamente autorizado y respaldado, por escrito, por la empresa prestadora de servicios y asistencia técnica de la marca ofertada en nuestro país (C.A.S.), quienes deberán contar con al menos 2 técnicos certificados. Se deberá presentar la nómina de técnicos certificados del CAS, con sus respectivas certificaciones.

#### **Para el Lote 3:**

- Los mantenimientos deberán ser brindados por personal certificado especializado de los equipos involucrados en esta contratación. El Oferente adjudicado deberá presentar los avaluos correspondientes, que indiquen que los mismos se encuentran en condiciones de llevar a cabo dichos servicios.
- El oferente deberá presentar certificación de 1 (Un) Técnico nivel Asociado de la marca ofertada.
- El oferente deberá presentar certificación de 01 (Un) Técnico nivel Profesional de la marca ofertada.
- El oferente deberá presentar certificación de 01 (Un) Técnico nivel Especialista de la marca ofertada.
- El oferente deberá presentar certificación de 01 (Un) profesional de nacionalidad paraguaya con certificación internacional con más de 7 años de vigencia en el nivel experto en redes informáticas.
- El oferente deberá presentar certificación de 01 (Un) técnico certificado a nivel profesional en Gestión de Proyectos (ITIL v4) o SCRUM Master o PMP que interactuará y dará soporte al personal asignado al proyecto.

#### **Para el Lote 4:**

- Catálogos, manual de equipo y otras documentaciones en español o inglés que respalde el cumplimiento con lo solicitado, indicando el ítem al cual corresponde.

## **Requisitos documentales para evaluar el criterio de capacidad técnica**

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

Declaración Jurada de tener Capacidad de brindar soporte técnico local en la República del Paraguay durante el periodo de garantía, de forma inmediata.
Certificación ISO 9001/2015 o similar, la similitud debe basarse en los mismos criterios que solicita o certifica la norma ISO 9001/2015 con respecto a la calidad de la gestión de procedimientos de Provisión e integración de bienes y/o servicios.
Declaración jurada en donde indique que dará cumplimiento a las garantías requeridas por el periodo de 36 meses.
Nota en la que liste nombre apellido y número de cedula de los técnicos certificados en las marcas mencionadas para cubrir los servicios contratados, adjuntar currículum y copia del certificado.
DD.JJ. que el personal asignado por la empresa Contratada se ceñirá a las normas y procedimientos de seguridad del Ministerio de Economía y Finanzas.
Declaración Jurada en que la Empresa se compromete a cumplir con todos los puntos solicitados en las Especificaciones Técnicas del PBC.
Los técnicos deberán estar en la planilla de IPS. Comprobada con constancia emitida por el IPS (Instituto de Previsión Social).
El Oferente debe demostrar experiencia en la provisión e instalación de Routers/Firewalls durante el periodo 2020 - 2023 demostrado de la siguiente manera: Copias de Facturaciones y/o contratos de haber proveído a Entidades Públicas y/o Privadas por lo menos el 50% (cincuenta por ciento) del monto de la oferta presentada.

**Para el Lote 1:**

**El oferente deberá contar con al menos:**

- 01 (uno) profesional con certificado vigente de PMP (Project Management Professional) certificado por el PMI (Project Manager Institute) o certificación vigente Scrum Master con reconocimiento internacional o certificaciones equivalentes, para la planificación, ejecución y control de los trabajos, Los cuales deberán ser verificable con la planilla de IPS y/o Estatuto de la empresa.
- 02 (dos) técnicos certificados por el fabricante de los equipos ofertados. La experiencia del personal en la solución ofertada deberá ser demostrable con la presentación del Certificado de Especialista emitido por el fabricante, demostrable con la planilla de IPS.
- 02 (dos) técnicos certificados en el producto de virtualización de Huawei Virtualization Suite Platinum Edition los cuales deben ser verificable con el formulario de inscripción y la última planilla de IPS.
- 02 (dos) técnicos certificados en Storage Huawei de nivel profesional con certificado vigente y verificable. La experiencia del personal debe ser demostrable con la presentación del Certificado de Especialista en Storage Huawei, el personal propuesto deba ser demostrable con la planilla de IPS y/o Estatuto de la empresa.
- 02 (dos) técnicos certificados en Veritas Backup Exec. la experiencia del personal deberá ser demostrable con la presentación del Certificado de Especialista en Veritas Backup, el personal propuesto deberá ser demostrable con la planilla de IPS y/o Estatuto de la empresa.

**Para el Lote 2:**

- El oferente deberá contar con al menos 2(dos) técnicos certificados en la marca ofertada, los mismos deberán estar inscriptos en IPS. Se deberá presentar última planilla vigente del Aporte Obrero Patronal IPS para garantizar que el personal propuesto pertenece a la nómina de funcionarios permanentes de la empresa. Además, será un requisito indispensable que la empresa oferente esté autorizada por el Fabricante a prestar el servicio técnico y el cambio de partes por garantía. Es también aceptable para la Convocante que el oferente esté debidamente autorizado y respaldado, por escrito, por la empresa prestadora de servicios y asistencia técnica de la marca ofertada en nuestro país (C.A.S.), quienes deberán contar con al menos 2 técnicos certificados. Se deberá presentar la nómina de técnicos certificados del CAS, con sus respectivas certificaciones.

**Para el Lote 3:**

- Los mantenimientos deberán ser brindados por personal certificado especializado de los equipos involucrados en esta contratación. El Oferente adjudicado deberá presentar los avales correspondientes, que indiquen que los mismos se encuentran en condiciones de llevar a cabo dichos servicios.
- El oferente deberá presentar certificación de 1 (Un) Técnico nivel Asociado de la marca ofertada.
- El oferente deberá presentar certificación de 01 (Un) Técnico nivel Profesional de la marca ofertada. El oferente deberá presentar certificación de 01 (Un) Técnico nivel Especialista de la marca ofertada.
- El oferente deberá presentar certificación de 01 (Un) profesional de nacionalidad paraguaya con certificación internacional con más de 7 años de vigencia en el nivel experto en redes informáticas.
- El oferente deberá presentar certificación de 01 (Un) técnico certificado a nivel profesional en Gestión de Proyectos (ITIL v4) o SCRUM Master o PMP que interactuará y dará soporte al personal asignado al proyecto.

**Para el Lote 4:**

- Catálogos, manual de equipo y otras documentaciones en español o inglés que respalde el cumplimiento con lo solicitado, indicando el ítem al cual corresponde.

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

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

DDJJ mediante el cual, el oferente se compromete en caso de ser adjudicado a contar con firma electrónica cualificada para la suscripción del respectivo contrato y todos los demás documentos relativos a la relación contractual, de conformidad con las normativas que rigen la firma electrónica (Ley N.º 6822/2021 "DE LOS SERVICIOS DE CONFIANZA PARA LAS TRANSACCIONES ELECTRÓNICAS, DEL DOCUMENTO ELECTRÓNICO Y LOS DOCUMENTOS

TRANSMISIBLES ELECTRÓNICOS, y su reglamentación, Decreto del Poder Ejecutivo N.º 7576/2022), como en virtud de lo establecido en la Ley N.º 6562/2020 DE LA REDUCCIÓN DE LA UTILIZACIÓN DE PAPEL EN LA GESTIÓN PÚBLICA Y SU REEMPLAZO POR EL FORMATO DIGITAL, conocida como Papel Cero, y su reglamentación, Decreto del Poder Ejecutivo N.º 4845/2021.

## **Aclaración de las ofertas**

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

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

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

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

## **Disconformidad, errores y omisiones**

Siempre y cuando una oferta se ajuste sustancialmente a las bases de la contratación, el Comité de Evaluación, requerirá que cualquier disconformidad u omisión que no constituya una desviación significativa, sea subsanada en cuanto a la información o documentación que permita al Comité de Evaluación realizar la calificación de la oferta.

A tal efecto, el Comité de Evaluación emplazará por escrito al oferente a que presente la información o documentación necesaria, dentro de un plazo razonable no menor a un día hábil, bajo apercibimiento de rechazo de la oferta. El Comité de Evaluación podrá reiterar el pedido cuando la respuesta no resulte satisfactoria, toda vez que no se viole el principio de igualdad.

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

- a) Si hay una discrepancia entre un precio unitario y el precio total obtenido al multiplicar ese precio unitario por las cantidades correspondientes, prevalecerá el precio unitario y el precio total será corregido.
- b) Si hay un error en un total que corresponde a la suma o resta de subtotales, los subtotales prevalecerán y se corregirá el total.
- c) En caso que el oferente haya cotizado su precio en guaraníes con décimos y céntimos la convocante procederá a realizar el redondeo hacia abajo.

Si hay una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras a menos que la cantidad expresada en palabras corresponda a un error aritmético, en cuyo caso prevalecerán las cantidades en cifras de conformidad con los párrafos (a) y (b) mencionados.

## **Criterios de desempate de ofertas**

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

## **Criterios de Adjudicación**

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

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

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

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

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

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

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

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

---

## Notificaciones

Cuando la convocante opte por notificar la adjudicación a través del SICP, la notificación de la misma será realizada de manera automática, a los correos declarados en el Registro de Proveedores del Estado de los oferentes presentados. A efectos de la notificación oficial, solo serán considerados tales correos electrónicos. La notificación comprenderá la Resolución de la adjudicación, el informe de evaluación.

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

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

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

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

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

---

## Audiencia Informativa

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

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

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

# SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS

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

## Suministros y Especificaciones técnicas

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

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

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

El Proveedor tendrá derecho a rehusar responsabilidad por cualquier diseño, dato, plano, especificación u otro documento, o por cualquier modificación proporcionada o diseñada por o en nombre de la Contratante, mediante notificación a la misma de dicho rechazo.

## Identificación de la unidad solicitante y justificaciones

En este apartado la convocante deberá indicar los siguientes datos:

- **Nombre, cargo y dependencia de la institución de quien solicita el llamado a ser publicado:** José Luis Cabrera Portillo, Jefe de Departamento de Informática de la Coordinación de Recursos Administrativos de la Dirección General de Administración y Finanzas de la Gerencia General del Ministerio de Economía y Finanzas.
- **Justificación de la necesidad:** El departamento de Informática/CRA/DGAF/GG administra los equipos de Datacenter del MEF, por lo que es necesario renovar los equipos tanto de procesamiento, almacenamiento y comunicación para garantizar el correcto funcionamiento de los servicios ofrecidos por la DGAF.
- **Justificación de la planificación:** Este llamado será realizado una única vez.
- **Justificación las especificaciones técnicas establecidas:** Las Especificaciones Técnicas se realizaron conforme a las necesidades de la institución, sugerencias y recomendaciones de las auditorías internas al Departamento de Informática.



**Especificaciones técnicas - CPS**

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

Especificaciones Técnicas			
Lote 1 Servidor para Clúster			
Descripción	Características		Mínimo Exigido
Marca	Indicar		Especificar
Modelo	Indicar		Especificar
Origen	Indicar		Especificar
Cantidad	Tres (03)		Exigido
Factor de Forma	Rackeable de 2U máximo.		Exigido
Procesador	Cantidad instalada en el equipo	02 (dos) de última generación con año de lanzamiento 2023 en adelante.	Exigido
	Cantidad máxima soportada por el equipo	2 (Dos) de última generación con año de lanzamiento 2023 en adelante.	Exigido
	Características de cada procesador	Cantidad de cores: 20 como mínimo.	Exigido
		Frecuencia: 2.0 GHz como mínimo.	Exigido
Memoria	Cantidad instalada	1TB como mínimo.	Exigido
	Tipo de memoria	DDR5 4800 MT/s LRDIMM como mínimo.	Exigido

	Capacidad máxima de memoria soportado por el equipo	4 TB como mínimo.	Exigido
	Cantidad máxima de slots soportados por el equipo	16 slots por procesador como mínimo.	Exigido
Módulo de Plataforma Segura	El equipo debe soportar TPM 2.0 mínimamente.		Exigido
Almacenamiento	2 (DOS) unidad SSD SATA Hot-Plug Lectura Intensiva de 960 GB o superior.		Exigido
	Capacidad de albergar hasta 8 discos SFF, con capacidad de crecimiento a 24 bahías a futuro.		Exigido
	El equipo debe poder soportar discos SAS, SATA y NVMe.		Exigido
	Controladora de discos	2 GB de cache tipo Flash o superior.	Exigido
		Soporte para RAID 0, 1, 10	Exigido
Ranuras de Expansión	2x16, 2x8 slots PCIe como mínimo.		Exigido
Interfaces de periféricos	Puertos USB: (04) cuatro unidades como mínimo versión 2.0		Exigido
	Puerto VGA: una unidad Los puertos deberán ser frontales o posteriores		Exigido
	Serial: con capacidad de poder agregar una unidad a futuro.		Exigido
Tarjeta Gráfica	Puerto grafico de 16MB integrado con resolución máxima de 1920x1200.		Exigido
Fuente de alimentación	Fuente de alimentación DUAL Redundante (1+1) platinum Hot Plug o similar		Exigido

Comunicaciones	2 (dos) puertos de 1GbE como mínimo.	Exigido
	2 (dos) puertos 10GB LAN (opticos) con sus SFP+ como mínimo.	Exigido
	2 (dos) puertos 10GB LAN (cobre) como mínimo.	Exigido
	2 (dos) puertos de 32GB FC con sus SFP como mínimo.	Exigido
Sistema Operativo Soportados	Windows Server 2016 o superior	Exigido
	Red Hat Enterprise Linux 7.0 o superior	Exigido
	Xenserver 7.1 o superior	Exigido
	Huawei DCS FusionCompute 8.0 o superior	Exigido
	VMware vSphere 7.0 o superior	Exigido
Características RAS	Diagnóstico de fallas de hardware en el equipo mediante LEDs indicadores. Además de luces LEDs indicadores de fallas, se requerirá que cuente con la descripción detallada de la alerta.	Exigido
Administración	Debe poseer puerto de consola dedicado y licenciamiento necesario para la administración remota del Servidor, que permita configurar, supervisar y actualizar el servidor. Debe poseer consola remota integrada y capacidad de montar medios virtuales.	Exigido
Kit de Montaje en Rack y Accesorios	Proporcionar el kit completo de: cables, soportes, organizadores y demás accesorios requeridos para el montaje y funcionamiento correcto del servidor en el rack.	Exigido
Montaje	Se deberá proveer el kit completo de montaje, cables, soportes, organizadores y demás accesorios requeridos para el montaje y funcionamiento correcto del servidor.	Exigido
Instalación	Todos los trabajos a ser ejecutados, deben ser presentados una vez terminados, de manera prolija y mecánicamente resistente.	Exigido

	Proveer los accesorios necesarios para la realización de las tareas: cintas, tornillos, arandelas, etc.	Exigido
	Además de cumplir con lo establecido en la presente documentación, las instalaciones deberán ser ejecutadas en un todo de acuerdo con los reglamentos para instalaciones de los estándares internacionales.	Exigido
Fabricación	Todos los equipos deben ser nuevos fabricación 2024 y de la última generación disponible del fabricante con fabricación reciente y encontrarse en comercialización activa	Exigido
Autorización	Carta de autorización del fabricante indicando que la empresa oferente es canal autorizado y está autorizado para presentar oferta para el presente llamado.	Exigido
Garantía	Carta de garantía del fabricante por 36 meses. El servicio de garantía deberá ser realizado por técnicos certificados avalado por el Fabricante.	Exigido
Plazo de entrega	60 (sesenta) días corridos desde la entrega de la orden de compra.	Exigido

	<p>El oferente deberá proveer los servicios profesionales necesarios para llevar a cabo de forma satisfactoria la migración de la infraestructura virtual Huawei DCS de su entorno de Producción del Ministerio de Economía y Finanzas a los nuevos servidores proveídos según requerimientos y para ello se solicita:</p> <p>La firma contratada deberá contar con al menos:</p> <p>01 (uno) profesional con certificado vigente de PMP (Project Management Professional) certificado por el PMI (Project Manager Institute) o certificación vigente Scrum Master con reconocimiento internacional o certificaciones equivalentes, para la planificación, ejecución y control de los trabajos, Los cuales deberán ser verificable con la planilla de IPS y/o Estatuto de la empresa.</p> <p>02 (dos) técnicos certificados por el fabricante de los equipos ofertados para la instalación física (rackeo) y configuración del arreglo raid.</p> <p>02 (dos) técnicos certificados en el producto de virtualización de Huawei Virtualization Suite Platinum Edition los cuáles serán los encargados de diseñar el nuevo esquema de la infraestructura virtual Huawei DCS y el procedimiento de migración de las VMs a los nuevos servidores del Ministerio de Economía y Finanzas.</p>	Exigido
Servicios e implementación	<p>También así realizarán la instalación de la Huawei DCS (la misma versión actualmente en producción) en los servidores nuevos.</p> <p>Deberá configurar en clúster de Huawei DCS los nuevos equipos con los mismos parámetros que actualmente está en producción el entorno virtual del Ministerio de Economía y Finanzas.</p> <p>Queda a cargo del oferente la correcta configuración de los equipos intermedios de comunicación (switches, routers, firewall, etc) para la migración y puesta en producción del nuevo clúster Huawei DCS con los equipos ofertados.</p> <p>Queda a cargo del oferente la correcta configuración de los switches SAN para la migración y puesta en producción del nuevo clúster Huawei DCS con los equipos ofertados.</p> <p>02 (dos) técnicos certificados en Storage Huawei de nivel profesional con certificado vigente y ID verificable los cuales serán los encargados de la creación de las LUNs necesarias para migrar y poner en producción las VM del nuevo entorno Huawei DCS. También estarán a cargo de configurar la funcionalidad Hypermetro (replica Activa-Activa entre Storage) que actualmente se encuentra en producción entre el datacenter de la DA y el datacenter de contingencia.</p> <p>02 (dos) técnicos certificados VCS Veritas Backup Exec 20.1 Administrator con certificado vigente y verificable los cuales serán los encargados de migrar y poner en producción los backup de las VM del nuevo entorno Huawei DCS.</p>	

Certificaciones técnicas	<p>El oferente deberá contar con al menos:</p> <p>01 (uno) profesional con certificado vigente de PMP (Project Management Professional) certificado por el PMI (Project Manager Institute) o certificación vigente Scrum Master con reconocimiento internacional o certificaciones equivalentes, para la planificación, ejecución y control de los trabajos, Los cuales deberán ser verificable con la planilla de IPS y/o Estatuto de la empresa.</p> <p>02 (dos) técnicos certificados por el fabricante de los equipos ofertados. La experiencia del personal en la solución ofertada deberá ser demostrable con la presentación del Certificado de Especialista emitido por el fabricante, demostrable con la planilla de IPS.</p> <p>02 (dos) técnicos certificados en el producto de virtualización de Huawei Virtualization Suite Platinum Edition los cuales deben ser verificable con el formulario de inscripción y la última planilla de IPS.</p> <p>02 (dos) técnicos certificados en Storage Huawei de nivel profesional con certificado vigente y verificable. La experiencia del personal debe ser demostrable con la presentación del Certificado de Especialista en Storage Huawei, el personal propuesto debera ser demostrable con la planilla de IPS y/o Estatuto de la empresa.</p> <p>02 (dos) técnicos certificados en Veritas Backup Exec. la experiencia del personal deberá ser demostrable con la presentación del Certificado de Especialista en Veritas Backup, el personal propuesto deberá ser demostrable con la planilla de IPS y/o Estatuto de la empresa.</p>	Exigido
Soporte	<p>El Oferente deberá contemplar el soporte técnico por un periodo de 36 meses.</p>	Exigido
	<p>Soporte on site 7 x 24 durante 3 (tres) años.</p>	Exigido

#### Lote 2 - Sistema de Almacenamiento - Storage

Descripción	Características	Mínimo Exigido
Marca	Especificar	Exigido
Modelo	Especificar	Exigido
Origen	Especificar	Exigido

<b>Cantidad</b>	1 (Uno)	Exigir
<b>Factor de forma</b>	Rackeable 19	Exigir
<b>Protocolos Front-End Soportados por el equipo.</b>	FC 16 Gbps	Exigir
	iSCSI 10 Gbps	Exigir
<b>Detalles del sistema de almacenamiento</b>	El sistema de almacenamiento debe incluir dos controladoras activas y redundantes entre sí.	Exigir
	Cada controladora debe contar con cuatro puertos FC 16 Gbps para conectividad Front-End.	Exigir
	Cada controladora debe contar con 384 GB de memoria caché como mínimo, totalizando 768GB. En caso de interrupción del fluido eléctrico, el equipo deberá contar con un mecanismo para mover la información de caché a disco con el fin de proteger la integridad de la información hasta que se reenergice el equipo.	Exigir
<b>Niveles de RAID</b>	El sistema de almacenamiento debe incluir la capacidad de definir arreglos de discos de nivel RAID 1, 5 y 6 como mínimo.	Exigir
<b>Capacidad entregada</b>	Inicial: Al menos 40TB de capacidad útil con discos NVMe SSD configurados en RAID 6	Exigir
	Se deberá proveer al menos 1 disco para spare	
<b>Tipos de discos soportados.</b>	NVMe SSD, SAS SSD y SAS HDD	Exigir
<b>Escalabilidad</b>	El equipo debe tener la posibilidad de crecer hasta por lo menos 5PB RAW internamente.	Exigir
<b>LUNs</b>	Tamaño máximo de LUN: 256TB o superior	Exigir
	Cantidad máxima de LUNs que permite realizar el Storage: 20.000 o superior	
<b>IOPS</b>	El dispositivo de almacenamiento deberá soportar al menos 3.500.000 de IOPS.	
<b>Software de Análisis y Reporte del desempeño</b>	El equipo ofertado deberá tener un software con la funcionalidad de enviar reportes ante cualquier eventualidad de fallo que fuera a tener el mismo. El equipo deberá estar configurado de modo a que el reporte generado sea enviado al proveedor y al fabricante al mismo tiempo de manera inmediata, para la posterior solución de la falla por parte del proveedor	Exigir

<b>Software de copia y replicación.</b>	El sistema debe poder ser capaz de realizar copias de los volúmenes dentro del mismo sistema de almacenamiento (Snapshots y Clones). Dicha funcionalidad debe ser incluida en caso de ser una licencia adicional. La licencia debe cubrir la capacidad total de crecimiento del dispositivo de almacenamiento	Exigir
<b>Software de Aprovisionamiento</b>	El sistema debe incluir el licenciamiento de software especializado que permita la provisión de capacidad física de almacenamiento en forma dinámica, la capacidad asignada no se deberá alojar en cuanto se cree el volumen, se deberá provisionar en cuanto la data sea efectivamente escrita en el volumen. (Thin- Provisioning)	Exigir
<b>Disponibilidad de componentes</b>	Las controladoras, discos, fuentes de poder y ventiladores deben ser hot-swap.	Exigir
	Las controladoras, fuentes de poder y ventilación deben ser redundantes.	Exigir
<b>Sistemas operativos de hosts compatibles</b>	Microsoft Windows Server	Exigir
	Red Hat Enterprise Linux	Exigir
	VMware	Exigir
	AIX	Exigir
	Huawei DCS	Exigir
<b>Técnicos y certificaciones</b>	El oferente deberá contar con al menos 2(dos) técnicos certificados en la marca ofertada, los mismos deberán formar parte de la nómina permanente de funcionarios de la empresa inscriptos en IPS. Se deberá presentar última planilla vigente del Aporte Obrero Patronal IPS para garantizar que el personal propuesto pertenece a la nómina de funcionarios permanentes de la empresa. Además, será un requisito indispensable que la empresa oferente esté autorizada por el Fabricante a prestar el servicio técnico y el cambio de partes por garantía. Es también aceptable para la Convocante que el oferente esté debidamente autorizado y respaldado, por escrito, por la empresa prestadora de servicios y asistencia técnica de la marca ofertada en nuestro país (C.A.S.), quienes deberán contar con al menos 2 técnicos certificados. Se deberá presentar la nómina de técnicos certificados del CAS, con sus respectivas certificaciones.	Exigir
<b>Experiencia</b>	La empresa oferente deberá acreditar al menos 5 instalaciones de Storage o similares a la ofertada (atendiendo siempre que sea de la misma marca, aunque pueda variar los modelos) dentro del territorio nacional, avalados por la correspondiente factura emitida en su oportunidad y una carta de conformidad del cliente relacionado a la recepción del equipo instalado. Además, se debe presentar adjunto a cada factura, información del número telefónico de contacto y la convocante se reserva el derecho de realizar una visita al Cliente referenciado.	Exigir
<b>Instalación</b>	El dispositivo de almacenamiento deberá ser instalado en un Rack indicado por la convocante y se deberá prever los kits necesarios para el rackeo	Exigir
<b>Autorización del fabricante</b>	El oferente deberá contar con Autorización del Representante Local de la marca en Paraguay, quien a su vez deberá estar avalado por el Fabricante.	Exigir



<b>Garantía</b>	3 (tres) años On Site. El servicio de garantía deberá ser realizado por técnicos certificados del CAS (Centro Autorizado de Servicios) avalado por el Fabricante.	Exigir
<b>Plazo de entrega</b>	El equipo deberá ser entregado 60 (sesenta) días posteriores a la recepción de la Orden de Compra correspondiente.	Exigir

#### Lote 3 Equipos de comunicación

##### Ítem 1 - Firewall de Borde

	Características	Requerido
<b>Cantidad</b>	1 (Uno)	
<b>Marca</b>	Especificar	
<b>Modelo</b>	Especificar	
<b>Origen/Procedencia</b>	Especificar	

Componente	Características	
<b>Características Equipo</b>	Throughput de por lo menos 20 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6	SI
	Soporte a por lo menos 7.5M conexiones simultaneas	SI
	Soporte a por lo menos 450K nuevas conexiones por segundo	SI
	Throughput de al menos 50 Gbps de VPN IPSec	SI
	Estar licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos	SI
	Estar licenciado para, o soportar sin necesidad de licencia, 15K túneles de clientes VPN IPSec simultáneos	SI
	Throughput de al menos 1 Gbps de VPN SSL	SI
	Soportar al menos 500 clientes de VPN SSL simultáneos	SI

	Soportar al menos 11 Gbps de throughput de IPS	SI
	Soportar al menos 1 Gbps de throughput de Inspección SSL	SI
	Soportar al menos 20 Gbps de throughput de Application Control	SI
	Soportar al menos 5 Gbps de throughput de NGFW	SI
	Soportar al menos 4 Gbps de throughput de Threat Protection	SI
	Permitir gestionar al menos 128 Access Points	SI
	Tener al menos 12 interfaces 1Gbps RJ45 y 4 interfaces SFP	SI
	Tener al menos 2 interfaces 10Gbps	SI
	Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance	SI
	Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance	SI
<b>Características Generales</b>	La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.;	SI
	Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;	SI
	Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;	SI
	La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;	SI
	Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación;	SI

La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;	SI
Los dispositivos de protección de red deben soportar 4000 VLANs Tags 802.1q;	SI
Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;	SI
Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;	SI
Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);	SI
Los dispositivos de protección de red deben soportar DHCP Relay;	SI
Los dispositivos de protección de red deben soportar DHCP Server;	SI
Los dispositivos de protección de red deben soportar sFlow;	SI
Los dispositivos de protección de red deben soportar Jumbo Frames;	SI
Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;	SI
Debe ser compatible con NAT dinámica (varios-a-1);	SI
Debe ser compatible con NAT dinámica (muchos-a-muchos);	SI
Debe soportar NAT estática (1-a-1);	SI
Debe admitir NAT estática (muchos-a-muchos);	SI
Debe ser compatible con NAT estático bidireccional 1-a-1;	SI
Debe ser compatible con la traducción de puertos (PAT);	SI
Debe ser compatible con NAT Origen;	SI

Debe ser compatible con NAT de destino;	SI
Debe soportar NAT de origen y NAT de destino de forma simultánea;	SI
Debe soportar NAT de origen y NAT de destino en la misma política	SI
Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;	SI
Debe ser compatible con NAT64 y NAT46;	SI
Debe implementar el protocolo ECMP;	SI
Debe soportar SD-WAN de forma nativa	SI
Debe soportar el balanceo de enlace hash por IP de origen;	SI
Debe soportar el balanceo de enlace por hash de IP de origen y destino;	SI
Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;	SI
Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;	SI
Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;	SI
Enviar logs a sistemas de gestión externos simultáneamente;	SI
Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;	SI
Debe incluir el registro y análisis centralizado de basado en la nube.	SI

De incluir el almacenamiento de registro y análisis centralizados basados en la nube como mínimo de 5Gb por día.	SI
Debe soportar protección contra la suplantación de identidad (anti-spoofing);	SI
Implementar la optimización del tráfico entre dos dispositivos;	SI
Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);	SI
Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);	SI
Soportar OSPF graceful restart;	SI
Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;	SI
Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;	SI
Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;	SI
Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;	SI
Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;	SI
Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;	SI
Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el clúster;	SI
La configuración de alta disponibilidad debe sincronizar: Sesiones;	SI
La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;	SI

La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;	SI
La configuración de alta disponibilidad debe sincronizar: Tablas FIB;	SI
En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;	SI
Debe soportar la creación de sistemas virtuales en el mismo equipo;	SI
Para una alta disponibilidad, el uso de clústeres virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;	SI
Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;	SI
La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;	SI
Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);	SI
Debe soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;	SI
El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;	SI
Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;	SI
La consola de administración debe soportar como mínimo, inglés, español y portugués.	SI

	La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad	SI
	La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas.	SI
<b>Control por Política de Firewall</b>	Debe soportar controles de zona de seguridad;	SI
	Debe contar con políticas de control por puerto y protocolo;	SI
	Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;	SI
	Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;	SI
	Firewall debe poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad;	SI
	Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;	SI
	Debe soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.	SI
	Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);	SI
	Debe soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes	SI
	Debe soportar el protocolo estándar de la industria VXLAN;	SI
	La solución debe permitir la implementación sin asistencia de SD-WAN	SI

Control de Aplicación	En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN;	SI
	la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.	SI
	Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;	SI
	Detección de miles de aplicaciones en 18 categorías, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;	SI
	Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;	SI
	Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;	SI
	Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de paquets para permitir la identificación de firmas de la aplicación conocidas por el fabricante;	SI
	Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;	SI
	Actualización de la base de firmas de la aplicación de forma automática;	SI
	Limitar el ancho de banda utilizado por las aplicaciones, basado en IP, por política de usuarios y grupos;	SI
	Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;	SI



	Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;	SI
	El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;	SI
	Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc.) permitiendo granularidad de control/reglas para el mismo;	SI
	Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;	SI
	Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo, permitir a Hangouts el chat pero impedir la llamada de video;	SI
	Debe permitir la diferenciación de aplicaciones Proxis (psiphon, Freerate, etc.) permitiendo granularidad de control/reglas para el mismo;	SI
	Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc);	SI
	Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;	SI
	Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;	SI
	Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente	SI
<b>Prevención de Amenazas</b>	Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;	SI
	Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);	SI

Las características de IPS y antivirus deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;	SI
Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;	SI
Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;	SI
Deber permitir el bloqueo de vulnerabilidades y exploits conocidos	SI
Debe incluir la protección contra ataques de denegación de servicio;	SI
Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;	SI
Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;	SI
Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;	SI
Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;	SI
Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);	SI
Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP , UDP, etc;	SI
Detectar y bloquear los escaneos de puertos de origen;	SI
Bloquear ataques realizados por gusanos (worms) conocidos;	SI
Contar con firmas específicas para la mitigación de ataques DoS y DDoS;	SI

Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);	SI
Debe poder crear firmas personalizadas en la interfaz gráfica del producto;	SI
Identificar y bloquear la comunicación con redes de bots;	SI
Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;	SI
Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;	SI
Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;	SI
Los eventos deben identificar el país que origino la amenaza;	SI
Debe incluir protección contra virus en contenido HTML y JavaScript, software espía (spyware) y gusanos (worms);	SI
Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;	SI
Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;	SI
En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;	SI
Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);	SI

<b>Filtrado de URL</b>	Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);	SI
	Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;	SI
	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;	SI
	Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;	SI
	Tener por lo menos 75 categorías de URL;	SI
	Debe tener la funcionalidad de exclusión de URLs por categoría;	SI
	Permitir página de bloqueo personalizada;	SI
	Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);	SI
<b>Identificación de Usuarios</b>	Además del Explicit Web Proxy, soportar proxy web transparente;	SI
	Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-directorio y base de datos local;	SI
	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios;	SI
	Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/controles basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc.;	SI

	Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / controles basados en usuarios y grupos de usuarios;	SI
	Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en las políticas/controles basados en usuarios y grupos de usuarios;	SI
	Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autenticación residente en el equipo de seguridad (portal cautivo);	SI
	Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;	SI
	Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;	SI
	Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;	SI
	Debe incluir al menos dos tokens de forma nativa, lo que permite la autenticación de dos factores;	SI
<b>QoS Traffic Shaping</b>	Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;	SI
	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;	SI
	Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;	SI
	Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;	SI
	Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;	SI

	Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;	SI
	En QoS debe permitir la definición de tráfico con ancho de banda garantizado;	SI
	En QoS debe permitir la definición de tráfico con máximo ancho de banda;	SI
	En QoS debe permitir la definición de colas de prioridad;	SI
	Soportar marcación de paquetes DiffServ, incluso por aplicación;	SI
	Soportar la modificación de los valores de DSCP para Diffserv;	SI
	Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);	SI
	Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;	SI
<b>Filtro de Datos</b>	Permite la creación de filtros para archivos y datos predefinidos;	SI
	Los archivos deben ser identificados por tamaño y tipo;	SI
	Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo identificados en las aplicaciones;	SI
	Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;	SI
	Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;	SI
	Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares;	SI
<b>Geo Localización</b>	Soportar la creación de políticas por geo-localización, permitiendo bloquear el tráfico de cierto País/Países;	SI

	Debe permitir la visualización de los países de origen y destino en los registros de acceso;	SI
	Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;	SI
VPN	Soporte VPN de sitio-a-sitio y cliente-a-sitio;	SI
	Soportar VPN IPSec;	SI
	Soportar VPN SSL;	SI
	La VPN IPSec debe ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512	SI
	La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;	SI
	La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);	SI
	La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);	SI
	Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;	SI
	Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;	SI
	Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;	SI
	Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;	SI
	Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;	SI

	Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;	SI
	Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;	SI
	Deberá mantener una conexión segura con el portal durante la sesión;	SI
	El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS.	SI
<b>Wireless Controller</b>	Solución de red inalámbrica que administre y controle de manera centralizada los puntos de acceso (AP);	SI
	Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;	SI
	Debe permitir la conexión de dispositivos inalámbricos que implementen los estándares IEEE 802.11a / b / g / n / ac y que transmitan tráfico IPv4 e IPv6 a través del controlador;	SI
	La solución debe ser capaz de administrar puntos de acceso de tipo indoor y outdoor;	SI
	El controlador inalámbrico debe permitir ser descubierto automáticamente por los puntos de acceso a través de Broadcast, DHCP y consulta DNS;	SI
	La solución debe optimizar el rendimiento y la cobertura inalámbrica (RF) en los puntos de acceso administrados por ella, realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. La solución debe permitir además deshabilitar el ajuste automático de potencia y canales cuando sea necesario;	SI
	Permitir programar día y hora en que ocurrirá la optimización del aprovisionamiento automático de canales en los Access Points;	SI
	El encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser tunelados hasta el controlador inalámbrico;	SI
	Cuando tunelado, el tráfico debe ser encriptado a través de DTLS o IPSEC;	SI



Debe permitir la administración de puntos de acceso conectados remotamente a través de WAN. En este escenario el encaminamiento de tráfico de los dispositivos conectados a la red inalámbrica debe ocurrir de forma distribuida (local switching), o sea, el tráfico debe ser cambiado localmente en la interfaz LAN del punto de acceso y no necesitará de tunelamiento hasta el controlador inalámbrico;	SI
Cuando el tráfico se conmuta directamente en los puertos Ethernet de los puntos de acceso (local switching) y la autenticación sea WPA/WPA2-Personal (PSK), en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica;	SI
La solución debe permitir definir qué redes serán tuneladas hasta la controladora y qué redes serán conmutadas directamente por la interfaz del punto de acceso;	SI
La solución debe soportar el recurso de Split-Tunneling de forma que sea posible definir, a través de las subredes de destino, qué paquetes serán tunelados hasta el controlador y cuáles serán conmutados localmente en la interfaz del punto de acceso;	SI
La solución debe implementar recursos que posibiliten la identificación de interferencias provenientes de equipos que operen en las frecuencias de 2.4GHz y 5GHz;	SI
La solución debe detectar Receiver Start of Packet (RX-SOP) en paquetes inalámbricos y ser capaz de omitir aquellos que están por debajo de determinado umbral especificado en dBm;	SI
La solución debe permitir el equilibrio de carga de los usuarios conectados a la infraestructura inalámbrica de forma automática. La distribución de los usuarios entre los puntos de acceso cercanos debe ocurrir sin intervención humana y basada en criterios como número de dispositivos asociados en cada punto de acceso;	SI
La solución debe tener mecanismos para detectar y mitigar los puntos de acceso no autorizados, también conocidos como Rogue AP. La mitigación debe realizarse de forma automática y batida en criterios tales como: intensidad de señal o SSID. Los puntos de acceso administrados por la solución deben evitar la conexión de clientes en puntos de acceso no autorizados;	SI
La solución debe identificar automáticamente puntos de acceso intrusos que estén conectados a la red de cable (LAN). La solución debe ser capaz de identificar el punto de acceso intruso incluso cuando el MAC Address de la interfaz LAN es ligeramente diferente (adyacente) del MAC Address de la interfaz WLAN;	SI

La solución debe detectar los puntos de acceso no autorizados y / o intrusos a través de radios dedicados a la función de análisis o a través de Off-channel / Background scanning. Cuando se realiza a través de Off-channel / Background scanning, la solución debe ser capaz de identificar el uso del punto de acceso para, en caso necesario, retrasar el análisis y de esta forma no perjudicar a los clientes conectados;	SI
La solución debe permitir la configuración individual de las radios del punto de acceso para que operen en el modo monitor, o sea, con función dedicada para detectar amenazas en la red inalámbrica y con ello permitir mayor flexibilidad en el diseño de la red;	SI
La solución debe permitir la adición de controlador redundante operando en N + 1. En este modo, el controlador redundante debe monitorear la disponibilidad y sincronizar la configuración del principal, además de asumir todas las funciones en caso de error del controlador principal. De esta forma, todos los puntos de acceso deben asociarse automáticamente al controlador redundante que pasará a tener función de primario de forma temporal;	SI
La solución debe permitir el agrupamiento de VLANs para que se distribuyan múltiples subredes en un determinado SSID, reduciendo así el broadcast y aumentando la disponibilidad de direcciones IP;	SI
La solución debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red. Debe ser posible especificar en qué puntos de acceso o grupos de puntos de acceso que cada dominio estará habilitado;	SI
La solución debe garantizar al administrador de la red determinar los horarios y días de la semana que las redes (SSID) estarán disponibles para los usuarios;	SI
Debe permitir restringir el número máximo de dispositivos conectados por punto de acceso y por radio;	SI
La solución debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming;	SI
La solución debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute la itinerancia;	SI

La solución debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectada mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos;	SI
La solución debe implementar el estándar IEEE 802.11w para prevenir ataques a la infraestructura inalámbrica;	SI
La solución debe soportar priorización a través de WMM y permitir la traducción de los valores a DSCP cuando los paquetes se destinan a la red de cableado;	SI
La solución debe implementar técnicas de Call Admission Control para limitar el número de llamadas simultáneas;	SI
La solución debe mostrar información sobre los dispositivos conectados a la infraestructura inalámbrica e informar al menos la siguiente información: Nombre de usuario conectado al dispositivo, Fabricante y sistema operativo del dispositivo, Dirección IP, SSID al que está conectado, Punto de acceso al que está conectado, Canal al que está conectado, Banda transmitida y recibida (en Kbps), intensidad de la señal considerando el ruido en dB (SNR), capacidad MIMO y horario de la asociación;	SI
Para garantizar una mejor distribución de dispositivos entre las frecuencias disponibles y mejorar la utilización de la radiofrecuencia, la solución debe ser capaz de distribuir automáticamente los dispositivos de banda dual para que se conecten primariamente a 5GHz a través del recurso conocido como Band Steering;	SI
La solución debe permitir la configuración de los data rates que se activarán en la herramienta y las que se deshabilitan para las frecuencias de 2.4 y 5GHz y los estándares 802.11a / b / g / n / ac;	SI
La solución debe tener capacidad capaz de convertir paquetes Multicast en paquetes Unicast cuando se reenvían a los dispositivos que están conectados a la infraestructura inalámbrica, mejorando así el consumo de Airtime;	SI
La solución debe soportar la característica que ignore Probe Requests de clientes que tienen una señal débil o distante. Debe permitir definir el umbral para que los Probe Requests sean ignorados;	SI
La solución debe permitir la configuración del valor de Short Guard Interval para 802.11n y 802.11ac en 5GHz;	SI

La solución debe implementar una característica conocida como Airtime Fairness (ATF) para controlar el uso de airtime asignando porcentajes a utilizar en los SSID;	SI
La solución debe implementar reglas de firewall (stateful) para controlar el tráfico permitiendo o descartando paquetes de acuerdo con la política configurada, reglas que deben utilizar como criterio direcciones de origen y destino (IPv4 e IPv6), puertos y protocolos;	SI
La solución debe implementar la función de web filtering para controlar los sitios que se accede a la red inalámbrica. Debe poseer una base de conocimiento para categorizar los sitios y permitir configurar qué categorías de sitios serán permitidos y bloqueados para cada perfil de usuario y SSID;	SI
La solución debe tener capacidad de reconocimiento de aplicaciones a través de la técnica de DPI (Deep Packet Inspection) que permita al administrador de la red monitorear el perfil de acceso de los usuarios e implementar políticas de control. Debe permitir el funcionamiento de esta característica y la actualización periódica de la base de aplicaciones durante todo el período de garantía de la solución;	SI
La base de reconocimiento de aplicaciones a través de DPI debe identificar con al menos 1500 (mil y quinientas) aplicaciones;	SI
La solución debe permitir la creación de reglas para el bloqueo y el límite de banda (en Mbps, Kbps ou Bps) para las aplicaciones reconocidas a través de la técnica de DPI;	SI
La solución debe, a través de la técnica de DPI, reconocer aplicaciones sensibles al negocio y permitir la priorización de este tráfico con QoS;	SI
La solución debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica. Al menos los siguientes ataques deben ser identificados: - Ataques de flood contra el protocolo EAPOL (EAPOL Flooding); - Los siguientes ataques de denegación de servicio: Association Flood, Authentication Flood, Broadcast Deauthentication y Spoofed Deauthentication; - ASLEAP; - Null Probe Response / Null SSID Probe Response; - Long Duration; - Ataques contra Wireless Bridges; - Weak WEP; - Invalid MAC OUI.	SI

La solución debe implementar mecanismos de protección para mitigar ataques a la infraestructura inalámbrica. Al menos ataques de denegación de servicio deben ser mitigados por la infraestructura a través del envío de paquetes de deauthentication	SI
La solución debe implementar mecanismos de protección contra ataques de ARP Poisoning en la red inalámbrica;	SI
La solución debe monitorear y clasificar el riesgo de las aplicaciones accedidas por los clientes inalámbricos;	SI
Permitir configurar el bloqueo en la comunicación entre los clientes inalámbricos conectados a un SSID;	SI
Debe implementar la autenticación administrativa a través del protocolo RADIUS;	SI
En combinación con los puntos de acceso, la solución debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES);	SI
En combinación con los puntos de acceso, la solución debe ser compatible e implementar el método de autenticación WPA3;	SI
La solución debe permitir la configuración de múltiples claves de autenticación PSK para su uso en un SSID determinado;	SI
Cuando se utiliza la función de múltiples claves PSK, la solución debe permitir la definición de límite en cuanto al número de conexiones simultáneas para cada clave creada;	SI
La solución debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios basados en los atributos proporcionados por los servidores RADIUS;	SI
La solución debe implementar el mecanismo de cambio de autorización dinámica a 802.1X, conocido como RADIUS CoA (Change of Authorization) para autenticaciones 802.1X;	SI
La solución debe admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP;	SI

La solución debe implementar la característica de autenticación de los usuarios a través de la página web HTTPS, también conocido como Captive Portal. La solución debe limitar el acceso de los usuarios mientras éstos no informen las credenciales válidas para el acceso a la red;	SI
La solución debe permitir el hospedaje del captive portal en la memoria interna del controlador inalámbrico;	SI
La solución debe permitir la personalización de la página de autenticación, de forma que el administrador de red sea capaz de cambiar el código HTML de la página web con formato de texto e insertar imágenes;	SI
La solución debe permitir la recopilación del correo electrónico de los usuarios como método de autorización para ingreso a la red;	SI
La solución debe permitir que la página de autenticación se quede alojada en un servidor externo;	SI
La solución debe permitir el registro de cuentas para usuarios visitantes en la memoria interna. La solución debe permitir que sea definido un período de validez para la cuenta creada;	SI
La solución debe garantizar que los usuarios se autenticquen en el portal cautivo que utilice la dirección IPv6;	SI
La solución debe tener interfaz gráfica para administrar y gestionar las cuentas de usuarios visitantes, no permitiendo acceso a las demás funciones de administración de la solución;	SI
Después de la creación de un usuario visitante, la solución debe enviar las credenciales por e-mail al usuario registrado;	SI
La solución debe implementar la función de DHCP Server (IPv4 y IPv6) para facilitar la configuración de las redes de visitantes;	SI
La solución debe identificar automáticamente el tipo de equipo y sistema operativo utilizado por el dispositivo conectado a la red inalámbrica;	SI
La solución debe permitir que los usuarios puedan acceder a los servicios disponibles a través del protocolo Bonjour (L2) y que estén alojados en otras subredes, como AirPlay y Chromecast. Debe ser posible especificar en qué VLANs el servicio estará disponible;	SI

La solución debe permitir la configuración de redes Mesh entre los puntos de acceso administrados por ella;	SI
La solución debe permitir la configuración de red Mesh entre puntos de acceso indoor y outdoor;	SI
La solución debe permitir ser administrada a través de los protocolos HTTPS y SSH vía IPv4 e IPv6;	SI
La solución debe permitir el envío de los Logs a múltiples servidores externos de syslog;	SI
La solución debe permitir ser administrada a través del protocolo SNMP (v1, v2c y v3), además de emitir notificaciones a través de la generación de traps;	SI
La solución debe permitir que los softwares de gestión realicen consultas directamente en los puntos de acceso a través del protocolo SNMP;	SI
La solución debe incluir soporte para las RFC 1213 (MIB II) y RFC 2665 (Ethernet-like MIB);	SI
La solución debe permitir la captura de paquetes en la red inalámbrica y exportarlos en archivos en formato .pcap;	SI
La solución debe permitir la adición de planta baja del pavimento para ilustrar gráficamente la posición geográfica y el estado de operación de los puntos de acceso administrados por ella. Debe permitir la adición de plantas bajas en los siguientes formatos: JPEG, PNG, GIF o CAD;	SI
La solución debe presentar gráficamente la topología lógica de la red, representar los elementos de la red gestionados, además de información sobre los usuarios conectados con la cantidad de datos transmitidos y recibidos por ellos;	SI
La solución debe implementar la administración unificada y de forma gráfica para redes WiFi y redes cableadas;	SI
La solución debe permitir la actualización de firmware del controlador inalámbrico incluso cuando se conecta de forma remota;	SI
La solución debe permitir la identificación del firmware utilizado por cada punto de acceso administrado y permitir la actualización individualizada a través de interfaz gráfica;	SI

	La solución debe tener herramientas de diagnóstico y depuración;	SI
	La solución debe soportar la comunicación con elementos externos a través de las API;	SI
	La solución deberá ser compatible y administrar los puntos de acceso de este proceso;	SI
	El equipo debe contar con soporte, servicios y garantía del fabricante por 36 meses	SI
<b>Servicios y garantía</b>	Las capacidades UTM deben estar presentes en los equipos y será decisión del contratante su adquisición	SI
<b>Plazo de entrega</b>	El equipo deberá ser entregado 60(seenta) días posteriores a la recepción de la Orden de Compra correspondiente.	SI

Ítem 2 - Punto de Acceso - WIFI		
Componente	Características	Requerido
Cantidad	30 (treinta)	
Marca	Especificar	
Modelo	Especificar	
Origen/Procedencia	Especificar	
Características Equipo	Debe ser del tipo Indoor	SI
	Soportar 3 radios wireless + 1 radio BLE	SI
	Deberá soportar fuente de alimentación AC	SI
	Soportar 512 usuarios totales conectados	SI
	Implementar las tecnologías 802.11 a/b/g/n/ac/ax	SI



Operar en las frecuencias de 2.4 / 5 GHz	SI
Deberá operar en las bandas 2.4002.4835, 5.1505.250, 5.2505.350, 5.4705.725, 5.7255.850	SI
Implementar UL MU-MIMO 802.11ax mode y DL-MU-MIMO	SI
Implementar 802.11ax	SI
Soportar al menos 16 SSID simultáneos	SI
La radio 1 debe operar en 2.4 GHz 20/40 MHz (1024 QAM)	SI
La radio 2 debe operar en 5.0 GHz 20/40/80 MHz (1024 QAM)	SI
La radio 3 debe operar en 2.4GHz, 5.0GHz, 6GHz 20/40/80/160MHz (1024 QAM)	SI
La radio 1 debe soportar velocidad de datos de al menos 570 Mbps	SI
La radio 2 debe soportar velocidad de datos de al menos 1200 Mbps	SI
La radio 3 debe soportar velocidad de datos de al menos 2400 Mbps	SI
Deberá soportar un MTBF superior a 20000 horas	SI
El AP deberá contar con al menos una interfaz 10/100/1000 Base-T RJ45 y una interfaz 100/1000/2500 Base-T RJ45 las cuales deben soportar alimentación via PoE 802.3at	SI
Deberá operar en temperaturas entre 00 y 45 grados celsius y humedad entre 5 y 90% non-condensing	SI
Deberá soportar EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST	SI
Deberá soportar WPA™, WPA2™, and WPA3™ with 802.1x or preshared key, WEP, Web Captive Portal, MAC blocklist & allowlist	SI

	Deberá soportar los estándares IEEE 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h, 802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11u, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az	SI
	Deberá soportar los modos Local-Bridge, Tunnel, Mesh	SI
<b>Funcionalidades Generales</b>	Punto de acceso (AP) que permita el acceso de los dispositivos a la red a través de la wireless y que posea todas sus configuraciones centralizadas en controlador inalámbrico;	SI
	Debe soportar el modo de operación centralizado, o sea, su operación depende del controlador inalámbrico que es responsable de gestionar las políticas de seguridad, calidad de servicio (QoS) y monitoreo de la radiofrecuencia;	SI
	Debe identificar automáticamente el controlador inalámbrico al que se conectará;	SI
	Debe permitir administrarse remotamente a través de links WAN;	SI
	Debe poseer capacidad dual-band con radios 2.4GHz, 5GHz y 6 GHz operando simultáneamente, además de permitir configuraciones independientes para cada radio;	SI
	El tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser encapsulados hasta el controlador inalámbrico;	SI
	Cuando sea encapsulado, el tráfico debe ser encriptado a través de DTLS o IPSEC;	SI
	Debe permitir el tráfico de los dispositivos conectados a la red inalámbrica de forma distribuida (local switching), o sea, el tráfico debe ser conmutado localmente en la interfaz LAN del punto de acceso y no necesitará ser encapsulado hasta el controlador inalámbrico;	SI
	Cuando el tráfico sea distribuido y la autenticación con PSK, en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica;	SI

En conjunto con el controlador inalámbrico, debe optimizar el rendimiento y la cobertura inalámbrica (RF), realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados;	SI
Deberá soportar la funcionalidad de ajuste automático de potencia para extender la cobertura en caso de falla del punto de acceso vecino gerenciado por la misma controladora;	SI
Debe soportar mecanismos para la detección y mitigación de puntos de acceso no autorizados, también conocidos como Rogue APs;	SI
En conjunto con el controlador inalámbrico, debe implementar mecanismos de protección para identificar ataques a la infraestructura inalámbrica (wIDS / wIPS);	SI
En conjunto con el controlador inalámbrico, debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red;	SI
En conjunto con el controlador inalámbrico, debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios en función de los atributos proporcionados por los servidores RADIUS;	SI
Debe implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming;	SI
Debe implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute el roaming;	SI
Debe implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectadas mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos;	SI
Debe implementar el estándar IEEE 802.11e;	SI
Debe implementar el estándar IEEE 802.11h;	SI
El punto de acceso deberá soportar agregación de paquetes A-MPDU y A-MSDU;	SI

	El punto de acceso deberá soportar (LPDC) - Low Density Parity Check;	SI
	El punto de Acceso deberá soportar (MLD) - Maximum Likelihood Demodulation;	SI
	El Punto de Acceso deberá soportar metodo de diversidad (MRC) Maximum Ratio Combining;	SI
	Debe tener indicadores luminosos (LED) para indicación de estado;	SI
	Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada;	SI
	Debe poseer un certificado emitido por la Wi-Fi Alliance;	SI
<b>Capacidad Técnica del oferente</b>	El oferente deberá contar con herramientas de hardware y Software dedicadas para el diseño e implementación de la red Wireless. Se aceptarán las herramientas conocidas en la industria Wireless tales como; AirCheck G2 y/o Ekahau Survey y/o AirMagnet Survey PRO y/o Hamina Wireless Planner Network. Además se deberá presentar 1 (un) técnico con certificación vigente en la herramienta del tipo Diseñador de Red inalámbrica con capacidades de optimizar y solucionar problemas de WI-FI Enterprise.	SI
	La herramienta deberá poder generar la documentación correspondiente al diseño predictivo (Antes de la implementación) y Survey activo del sitio posterior a la implementación de la red Wireless, esto abrirá el camino al proceso de implementación real, donde el oferente deberá incluir información real medida del sitio a fin de ajustar la configuración para prevenir posibles interferencias tanto adyacentes de propios APs como externos	
	El Hardware de medición debe incorporar arreglos de antenas en 2,4/5/6 GHz como también un analizador de espectro en dichas frecuencias	SI
	Contar con 1 (un) Técnico Certificado del tipo Enterprise Wireless Implementación, para Implementar, proteger y configurar una infraestructura de red inalámbrica personalizada	SI
<b>garantía</b>	36 meses	SI

<b>Plazo de entrega</b>	El equipo deberá ser entregado 60(sesenta) días posteriores a la recepción de la Orden de Compra correspondiente.	SI
-------------------------	---	----

### Ítem 3 Clientes VPN y solución de Seguridad para estaciones de trabajo

Componente	Características	Requerido
<b>Cantidad</b>	500 (quinientas) estaciones de trabajo	
<b>Marca</b>	Especificar	
<b>Modelo</b>	Especificar	
<b>Origen/Procedencia</b>	Especificar	
<b>Funcionalidades generales</b>	Debe permitir gestión centralizada de endpoint	SI
	Debe permitir la gestión del cliente de seguridad de endpoint desde una consola central del fabricante	SI
	Debe permitir la configuración de perfiles en función de estados asignados por el servidor DHCP presente en el firewall de administración centralizada del mismo fabricante;	SI
	El licenciamiento debe estar basado en la cantidad de clientes registrados en la consola de gestión central del mismo fabricante	SI
	Debe ser compatible con los siguientes sistemas operativos: Microsoft Windows: 7 (32 y 64 bits), 8 (32 y 64 bits), 8.1 (32 y 64 bits), 10 (32 e 64 bits), 11(64 bits); Microsoft Windows Server: 2012 y superior; Mac OS: 10.14, 10.15 y 11+, IOS 9 o superior, Android 5 o superior, Linux Ubuntu 16.04 y superior, Red Hat 7.4 y superior, CentOS 7.4 y superior.	SI
	Debe tener interfaz gráfica de usuario al menos en el idioma inglés, portugués y español;	SI
	Debe permitir la copia de seguridad del archivo de configuración del endpoint	SI
	El cliente de seguridad debe poder generar bitácora (logs) sobre las funcionalidades instaladas y configuradas	SI

	Por lo menos los siguientes niveles de log deben estar disponibles: emergencia, alerta, crítico, error, aviso, informativo;	SI
	El cliente de seguridad debe poder enviar los registros (logs) a la consola de gestión central	SI
	El cliente de seguridad debe permitir la configuración local via XML (eXtensible Markup Language);	SI
	El cliente de seguridad debe poder integrarse con tecnologías de Sandboxing del mismo fabricante; la solución debe incluir la opción de suscripción de Sandbox sCloud	SI
<b>Funcionalidades de Provisionamiento de Clientes</b>	El fabricante debe proveer un portal para descargar el cliente seguridad y permitir la instalación local	SI
	Debe ser compatible con la instalación vía Active Directory de Microsoft	SI
	La consola de gestión central debe ser capaz de instalar el cliente de seguridad en computadoras Windows asociadas a un dominio Microsoft	SI
<b>Funcionalidades de Antivirus</b>	El cliente de seguridad debe ser capaz de inspeccionar archivos ejecutables, librerías y drivers en busca de virus	SI
	El cliente de seguridad debe ser capaz de buscar actualizaciones de firmas automáticamente	SI
	El cliente de seguridad debe ser capaz de enviar archivos para ser inspeccionados en sistemas de Sandboxing del mismo fabricante	SI
	El cliente de seguridad debe bloquear canales de comunicación usados por hackers o atacantes	SI
	El cliente de seguridad debe notificar localmente cuando se detecta un virus	SI
	El cliente de seguridad debe permitir que el usuario comience un escaneo bajo demanda	SI
	El cliente de seguridad debe permitir que se comience escaneo de virus de forma automática regularmente	SI

	El cliente de seguridad debe permitir visualizar los archivos puestos en cuarentena	SI
	Debe permitir la configuración del perfil antivirus desde la consola central del mismo fabricante	SI
	Debe permitir la configuración del perfil de filtro de web desde la consola central del mismo fabricante	SI
	El fabricante debe disponibilizar consultas en línea desde el cliente de seguridad sobre la categoría de determinada web (por ej. Interés general, tecnología, hacking, pornografía, etc.) para aplicar política de control de acceso a internet	SI
	El cliente de seguridad debe admitir reglas estáticas de acceso a internet basado en expresiones regulares	SI
	Para una URL determinadas las acciones deben ser: permitir, bloquear, alertar o monitorear	SI
<b>Funcionalidades de Firewall de Aplicación</b>	El cliente de seguridad debe admitir perfiles de Control de Aplicaciones creados centralmente desde la consola de gestión del mismo fabricante	SI
	El fabricante debe disponibilizar consultas en línea desde el cliente de seguridad sobre la categoría de determinada aplicación a modo de ser usada en la política de control de acceso	SI
	Debe ser reconocido más de 2800 aplicaciones por el cliente para ser usadas en reglas de control de acceso	SI
<b>Funcionalidades de VPN SSL</b>	Debe permitir que el usuario cree nuevas VPN SSL	SI
	Debe permitir que existan varias VPN SSL definidas simultáneamente	SI
	Debe permitir la personalización del puerto TCP en el que funciona la VPN SSL	SI
	Debe permitir la autenticación usando usuario y clave	SI
	Debe permitir la autenticación de dos factores provisto por el mismo fabricante	SI

	Debe permitir la autenticación usando certificados digitales	SI
<b>Funcionalidades de VPN IPsec</b>	Debe permitir que el usuario cree nuevas VPN IPSEC	SI
	Debe permitir que existan varias VPN IPSEC definidas simultáneamente	SI
	Debe permitir la autenticación usando usuario y clave	SI
	Debe permitir la autenticación usando certificados digitales	SI
	Debe permitir la selección de Modo Main y Agresivo;	SI
	Debe permitir la configuración de DHCP sobre IPsec;	SI
	Debe permitir el uso de NAT Traversal;	SI
	Debe permitir la elección de grupos Diffie-Hellman (1,2,5 e 14);	SI
	Debe permitir la configuración de expiración de claves IKE;	SI
	Debe permitir el uso de Perfect Forward Secrecy;	SI
	Debe permitir la autenticación de dos factores provisto por el mismo fabricante	SI
<b>Funcionalidades de la Solucion</b>	Debe gestionar de manera transparente para el usuario la selección del Gateway.	SI
	Debe gestionar la salud del Endpoint, la telemetría, la identidad del usuario y los certificados.	SI
	Debe continuamente chequear la postura de seguridad del endpoint.	SI
	Debe funcionar en modo Proxy para conexiones HTTPS y/o modo transparente TCP	SI
	Debe soportar integración con Multi Factor de Autenticacion	SI



	Debe brindar funcionalidades de (CASB) Cloud Access Security Broker en línea.	SI
<b>Funcionalidades de Scanner de Vulnerabilidades</b>	El cliente de seguridad debe tener integrado un módulo de búsqueda de vulnerabilidades y permitir la gestión central desde la consola del mismo fabricante	SI
	Debe permitir que el usuario comience un análisis de vulnerabilidades bajo demanda	SI
	Las vulnerabilidades encontradas deben ser mostradas localmente con un vínculo para visualizar información desde una base de datos en internet. Debe tener al menos: nombre, severidad y detalles	SI
<b>Funcionalidades de Gestión</b>	Debe permitir la instalación sobre Microsoft Windows Server 2012 o superior.	SI
	Debe permitir adicionar clientes mediante la adición de licencias	SI
	Debe tener interfaz de gestión gráfica	SI
	Debe tener la funcionalidad de backup	SI
	Debe permitir la creación de usuarios de diferente perfil administrativo	SI
	Debe permitir importar información desde Active Directory mediante LDAP	SI
	El registro manual de estaciones debe permitir el uso de clave	SI
	Debe permitir la creación de grupos de clientes para facilitar la gestión	SI
	Debe permitir la configuración de clientes mediante definición XML	SI
	Debe permitir la importación de configuración de perfiles desde firewall de mismo fabricante	SI
	Debe permitir configuración de diferentes grupos y perfiles para facilitar la administración	SI

Debe permitir la configuración de perfiles de antivirus, webfilter, control de aplicaciones, scanner de vulnerabilidades y VPN	SI
Debe permitir habilitar la protección en tiempo real	SI
Debe permitir configurar la búsqueda de virus y vulnerabilidades de forma programada	SI
Debe permitir ejecutar escaneo total y escaneo rapido	SI
Debe permitir configurar filtro de URLs provisto por el fabricante con al menos las siguientes acciones: bloquear, advertir, permitir y monitorar;	SI
Debe permitir configurar filtro de URLs basado en wildcards o expresiones regulares con las siguientes acciones: bloquear ou permitir;	SI
Debe permitir al usuario configurar VPNs localmente	SI
Debe permitir al usuario desconectar una VPN	SI
Debe permitir la conexión de VPN antes de login	SI
Debe permitir conexión automática de VPN	SI
Específico y general para VPN IPSec (al menos):	SI
Uso de certificados o usuario y clave para autenticación	SI
Uso de certificados en smartcard	SI
Verificación de checksum	SI
Bloqueo de tráfico IPv6	SI
Específico a SSL VPN (al menos):	SI
Especificación de la IP del concentrador	SI
Especificación del puerto del concentrador	SI

	Opción para que el usuario pueda acceder a la configuración del cliente mediante contraseña	SI
	Envío de logs hacia sistemas de logs externos del mismo fabricante	SI
	Registro junto al sistema de gerencia de forma silenciosa (de forma que sea no perceptible para el usuario);	SI
	Instalación de certificado digital en el cliente	SI
	Debe permitir habilitar funcionalidades de Single Sign On	SI
	El sistema de gestión central debe tener disponible información sobre: Cantidad de dispositivos gestionados, Versión de Sistema Operativo, Perfil aplicado, Usuario, Versión de firmas de Antivirus	SI
	Estado del cliente de seguridad: Registrado o no registrado	SI
	Información sobre el sistema operativo en el que está instalado el cliente	SI
	Perfil de seguridad creados y/o aplicados	SI
	Funcionalidades de seguridad aplicadas: antivirus, filtro web, VPN, firewall de aplicaciones;	SI
<b>garantía</b>	36 meses	SI
<b>Plazo de entrega</b>	La herramienta deberá ser entregado 60(seSENTA) días posteriores a la recepción de la Orden de Compra correspondiente.	SI

Ítem 4 -Analizador de tráfico y seguridad		
Componente	Características	Requerido
Cantidad	1 (Uno)	
Marca	Especificar	

<b>Modelo</b>	Especificar	
<b>Origen/Procedencia</b>	Especificar	
<b>Características del equipo</b>	La solución debe ser del tipo Virtual Appliance para implementarse on premise.	SI
	La solución no debe tener restricciones en la capacidad de almacenamiento en disco.	SI
	Debe recibir y procesar logs de todos los SDWAN y Next Generation Firewall solicitados en el presente pliego.	SI
<b>Licenciamiento</b>	La solución debe presentar un esquema de licenciamiento por suscripción.	SI
	Se debe licenciar la cantidad de GB por día de logs que puede recibir la solución.	SI
	La solución debe tener capacidad de recibir y procesar al menos 10 GB de logs diarios.	SI
	La suscripción debe incluir análisis de Indicadores de Compromisos, con inteligencia provista y actualizada periódicamente por el fabricante.	SI
	La suscripción debe incluir un dashboard de SoC donde se permitan realizar tareas automatizadas a partir de diversos inputs preconfigurados.	SI
<b>Requerimientos funcionales</b>	La solución debe permitir la virtualización en los siguientes hipervisores: VMware ESX/ESXi 5.5/6.0/6.5/6.7/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+ y KVM sobre Redhat 6.5+.	SI
	La solución no debe tener limitaciones en cuanto a la asignación de vCPU.	SI
	La solución no debe tener limitaciones en cuanto a la asignación de memoria.	SI
	Debe soportar acceso vía SSH, WEB (HTTPS) para la gestión de la solución.	SI

Contar con comunicación cifrada y autenticación con usuario y contraseña para su administración, tanto en interface gráfica (GUI) como vía línea de comandos.	SI
Permitir acceso simultáneo de administración, así como permitir crear por lo menos 2 (dos) perfiles para administración y monitoreo.	SI
Soporte SNMP versión 2 y 3.	SI
Debe permitir activar y desactivar para cada interface de la plataforma, los permisos de acceso HTTP, HTTPS, SSH.	SI
Debe permitir la autenticación de usuarios de acceso a la plataforma vía LDAP.	SI
Debe permitir la autenticación de usuarios de acceso a la plataforma vía Radius.	SI
Generación de informes en tiempo real de tráfico, en formato de gráfica de mapas geográficos.	SI
Generación de informes en tiempo real de tráfico, en formato de gráfica de burbuja.	SI
Generación de informes en tiempo real de tráfico, en formato de gráfica de tabla	SI
Definición de perfiles de acceso a consola con permiso granulares, tales como: acceso de escritura, de lectura, de creación de nuevos usuarios y cambios en configuraciones generales.	SI
Debe contar con un asistente gráfico para agregar nuevos dispositivos, usando la dirección IP, usuario y contraseña del mismo.	SI
Debe ser posible ver la cantidad de logs enviados desde cada dispositivo supervisado.	SI
Contar con mecanismos de borrado automático de logs antiguos.	SI
Permitir la importación y exportación de reportes.	SI

Debe contar con la capacidad de crear informes en formato HTML/PDF/XML/CSV.	SI
Debe permitir exportar los logs en formato CSV.	SI
Generación de logs de auditoría, con detalle de la configuración realizada, el administrador que realizó el cambio y hora del mismo.	SI
Los logs generados por los dispositivos administrados deben ser centralizados en los servidores de la plataforma, pero la solución debe ofrecer también la posibilidad de utilizar un servidor externo de Syslog o similar.	SI
La solución debe contar con reportes predefinidos.	SI
Debe poder enviar automáticamente los logs a un servidor FTP externo a la solución.	SI
Debe ser posible la duplicación de reportes existentes para su posterior edición.	SI
Debe tener la capacidad de personalizar la portada de los reportes obtenidos.	SI
Permitir centralmente la visualización de logs recibidos por uno o más dispositivos, incluido la capacidad de uso de filtros para facilitar la búsqueda dentro de los mismos logs.	SI
Los logs de auditoría de cambios de configuración de reglas y objetos deben ser visualizados en una lista distinta a la de los logs relacionados a tráfico de datos.	SI
Tener la capacidad de personalización de gráficas en los reportes, tales como barras, líneas y tablas.	SI
Debe poseer mecanismo de Drill-Down para navegar en los reportes de tiempo real.	SI
Tener la capacidad de generar y enviar reportes periódicos automáticamente.	SI
Permitir la personalización de cualquier reporte preestablecido por la solución, exclusivamente por el Administrador, para adoptarlo a sus necesidades.	SI

Permitir el envío por email de manera automática de reportes.	SI
Debe permitir que el reporte a enviar por email sea al destinatario específico.	SI
Permitir la programación de reportes, conforme a un calendario definido por el administrador.	SI
Debe ser posible visualizar gráficamente en tiempo real la tasa de generación de logs por cada dispositivo gestionado.	SI
Debe permitir el uso de filtros en los reportes.	SI
Debe permitir definir el diseño de los reportes, incluir gráfico, añadir texto e imágenes, alineación, saltos de página, fuentes, colores, entre otros.	SI
Permitir especificar el idioma de los reportes creados.	SI
Generar alertas automáticas vía email, SNMP y Syslog, basado en eventos especiales en logs, severidad del evento, entre otros.	SI
Debe permitir el envío automático de reportes a un servidor externo SFTP o FTP.	SI
Debe ser capaz de crear consultas SQL o similar dentro de las bases de datos de logs, para uso en gráficas y tablas en reportes.	SI
Tener la capacidad de visualizar en GUI de reportes de información del Sistema, como licencias, memoria, disco duro, uso de CPU, tasa de logs por segundo recibidos, total de logs diarios recibidos, alertas del sistema, entre otros.	SI
Debe contar con una herramienta que permita analizar el rendimiento en la generación de reportes, con el objetivo de detectar y arreglar problemas en generación de los mismos.	SI
Que la solución sea capaz de importar archivos con logs de dispositivos compatibles conocido y no conocidos por la plataforma, para posterior generación de reportes.	SI
Debe ser posible poder definir el espacio que cada instancia de virtualización puede utilizar para almacenamiento de logs.	SI

Debe proporcionar la información de cantidad de logs almacenados y la estadística de tiempo restante de almacenado.	SI
Debe ser compatible con autenticación de doble factor (token) para usuarios administradores de la plataforma.	SI
Debe permitir aplicar políticas para el uso de contraseñas para los administradores de la plataforma, como tamaño mínimo y caracteres permitidos	SI
Debe permitir visualizar en tiempo real los logs recibidos.	SI
Debe permitir el reenvío de logs en formato syslog.	SI
Debe permitir el reenvío de logs en formato CEF (Common Event Format).	SI
Debe incluir dashboard para operaciones SOC que monitorea las principales amenazas de seguridad para la red.	SI
Debe incluir dashboard para operaciones SOC que monitorea comprometimiento de usuarios y uso sospechoso de la web en la red.	SI
Debe incluir dashboard para operaciones SOC que monitorea el tráfico en la red.	SI
Debe incluir dashboard para operaciones SOC que monitorea el tráfico de aplicaciones y sitios web en la red.	SI
Debe incluir dashboard para operaciones SOC que monitorea detecciones de amenazas de día cero en la red (sandboxing).	SI
Debe incluir dashboard para operaciones SOC que monitorea actividad de endpoints en la red.	SI
Debe incluir dashboard para operaciones SOC que monitorea actividad VPN en la red.	SI
Debe incluir dashboard para operaciones SOC que monitorea puntos de acceso WiFi y SSIDs	SI
Debe incluir dashboard para operaciones SOC que monitorea rendimiento de recursos local de la solución (CPU, Memoria).	SI



Debe permitir crear dashboards personalizados para monitoreo de operaciones SOC.	SI
Debe soportar configuración de alta disponibilidad Master/Slave en la capa 3.	SI
Debe permitir generar alertas de eventos a partir de logs recibidos.	SI
Debe permitir crear incidentes a partir de alertas de eventos para endpoint.	SI
Debe permitir la integración al sistema de tickets ServiceNow.	SI
Debe soportar servicio de Indicadores de Compromiso (IoC) del mismo fabricante, que muestre las sospechas de comprometimiento de usuarios finales en la web, debiendo informar por lo menos: dirección IP de usuario, hostname, sistema operativo, veredicto (clasificación general de la amenaza), el número de amenazas detectadas.	SI
Debe soportar el estándar SAML para autenticación de usuarios administradores.	SI
Reportes de Firewall	SI
Debe contar con reporte de cumplimiento de PCI DSS	SI
Debe contar con reporte de utilización de aplicaciones SaaS	SI
Debe contar con reporte de prevención de pérdida de datos (DLP)	SI
Debe contar con reporte de VPN	SI
Debe contar con reporte de Sistema de prevención de intrusos (IPS)	SI
Debe contar con reporte de reputación de cliente	SI
Debe contar con reporte de análisis de seguridad de usuario	SI
Debe contar con reporte de análisis de amenaza cibernética	SI

	Debe contar con reporte de breve resumen diario de eventos e incidentes de seguridad	SI
	Debe contar con reporte de tráfico DNS	SI
	Debe contar con reporte tráfico de correo electrónico	SI
	Debe contar con reporte de Top 10 de Aplicaciones utilizadas en la red	SI
	Debe contar con reporte de Top 10 de Websites utilizadas en la red	SI
	Debe contar con reporte de uso de redes sociales	SI
<b>garantía</b>	36 meses	SI
<b>Plazo de entrega</b>	La herramienta deberá ser entregado 60(seSENTA) días posteriores a la recepción de la Orden de Compra correspondiente.	SI

### Capacitación para el Lote 3

El oferente para este lote debe incluir la capacitación de nivel Fundamental, Asociado y Profesional con instructores, materiales de estudio y laboratorios oficiales de la marca ofertada, se deberá prever para dos técnicos del Departamento de Informática.

### Capacidad Técnica para el Lote 3

-Los mantenimientos deberán ser brindados por personal certificado especializado de los equipos involucrados en esta contratación. El Oferente adjudicado deberá presentar los avales correspondientes, que indiquen que los mismos se encuentran en condiciones de llevar a cabo dichos servicios.

- El oferente deberá presentar certificación de 1 (Un) Técnico nivel Asociado de la marca ofertada.
- El oferente deberá presentar certificación de 01 (Un) Técnico nivel Profesional de la marca ofertada.
- El oferente deberá presentar certificación de 01 (Un) Técnico nivel Especialista de la marca ofertada.
- El oferente deberá presentar certificación de 01 (Un) profesional de nacionalidad paraguaya con certificación internacional con más de 7 años de vigencia en el nivel experto en redes informáticas.
- El oferente deberá presentar certificación de 01 (Un) técnico certificado a nivel profesional en Gestión de Proyectos (ITIL v4) o SCRUM Master o PMP que interactuará y dará soporte al personal asignado al proyecto.
- Los técnicos deberán estar en la planilla de IPS. Comprobada con constancia emitida por el IPS (Instituto de Previsión Social)

El Oferente debe demostrar experiencia en la provisión e instalación de Routers/Firewalls durante el periodo 2020 - 2023 demostrado de la siguiente manera: Copias de Facturaciones y/o contratos de haber proveído a Entidades Públicas y/o Privadas por lo menos el 50% (cincuenta por ciento) del monto de la oferta presentada.

### Autorización del fabricante para el Lote 3

Autorización del fabricante, con ID del llamado, se verificará al momento de la apertura de ofertas.

### Lote 4 Módulos SFP

Ítem 1 - Módulo SFP para fibra óptica Mono Modo (SMF)		
Componente	Características	Requerido
Cantidad	10 (Diez)	SI
Marca	Especificar	SI
Modelo	Especificar	SI
Origen/Procedencia	Especificar	SI
Velocidad de datos	10Gbps	SI
Longitud de onda	1310nm	SI
Conector	LC Dúplex	SI
Distancia de Cable	10 Km	SI
Factor de forma	Small Form-Factor Pluggable (SFP)	SI
Plataformas compatibles	Cisco ASR 1000 Series Router, Cisco Catalyst 3850 Series Switches, Cisco Catalyst 4500 and 4500-X Series Switches, Cisco Catalyst 2960-X Series Switches	SI
Garantía	12 meses	SI
Plazo de entrega	Deberá ser entregado 30(treinta) días posteriores a la recepción de la Orden de Compra correspondiente.	SI

Ítem 2 -Módulo SFP para fibra óptica Multi Modo (MMF)		
Componente	Características	Requerido
Cantidad	8 (Ocho)	SI
Marca	Especificar	SI

<b>Modelo</b>	Especificar	SI
<b>Origen/Procedencia</b>	Especificar	SI
<b>Velocidad de datos</b>	10Gbps	SI
<b>Longitud de onda</b>	850nm	SI
<b>Conector</b>	LC Duplex	SI
<b>Distancia de cable</b>	300m	SI
<b>Factor de forma</b>	Small Form-Factor Pluggable (SFP)	SI
<b>Plataformas compatibles</b>	Cisco ASR 1000 Series Router, Cisco Catalyst 3850 Series Switches, Cisco Catalyst 4500 and 4500-X Series Switches, Cisco Catalyst 2960-X Series Switches	SI
<b>Garantía</b>	12 meses	SI
<b>Plazo de entrega</b>	Deberá ser entregado 30(treinta) días posteriores a la recepción de la Orden de Compra correspondiente.	SI

Ítem 3 - Módulo SFP para fibra óptica Multi Modo (MMF)		
Componente	Características	Requerido
<b>Cantidad</b>	6 (Seis)	SI
<b>Marca</b>	Especificar	SI
<b>Modelo</b>	Especificar	SI
<b>Origen/Procedencia</b>	Especificar	SI
<b>Velocidad de datos</b>	1Gbps	SI

<b>Longitud de onda</b>	850nm	SI
<b>Conector</b>	LC Duplex	SI
<b>Distancia de cable</b>	300m	SI
<b>Factor de forma</b>	Small Form-Factor Pluggable (SFP)	SI
<b>Plataformas compatibles</b>	Cisco ASR 1000 Series Router, Cisco Catalyst 3850 Series Switches, Cisco Catalyst 4500 and 4500-X Series Switches, Cisco Catalyst 2960-X Series Switches	SI
<b>Garantía</b>	12 meses	SI
<b>Plazo de entrega</b>	Deberá ser entregado 30(treinta) días posteriores a la recepción de la Orden de Compra correspondiente.	SI

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

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

- Las EETT deberán especificar todas las características y requisitos técnicos esenciales y de funcionamiento, incluyendo los valores máximos o mínimos aceptables o garantizados, según corresponda. Cuando sea necesario, la convocante deberá incluir un formulario específico adicional de oferta (como un Anexo al Formulario de Presentación de la Oferta), donde el oferente proporcionará la información detallada de dichas características técnicas o de funcionamiento con relación a los valores aceptables o garantizados.

Cuando la convocante requiera que el oferente proporcione en su oferta una parte de o todas las Especificaciones Técnicas, cronogramas técnicos, u otra información técnica, la convocante deberá especificar detalladamente la naturaleza y alcance de la información requerida y la forma en que deberá ser presentada por el oferente en su oferta.

Si se debe proporcionar un resumen de las EETT, la convocante deberá insertar la información en la tabla siguiente. El oferente preparará un cuadro similar para documentar el cumplimiento con los requerimientos.

## Detalle de los bienes y/o servicios

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

Lote	Ítem	Descripción	Cantidad
1	1	Servidor para clúster	3
2	1	Sistema de Almacenamiento - Storage	1
3	Equipos de comunicación		
	1	Firewall de Borde	1
	2	Punto de Acceso - WIFI	30
	3	Cliente VPN y solución de seguridad para estaciones de trabajo	500
	4	Analizador de tráfico y Seguridad	1
4	Módulos SFP		
	1	Módulo SFP para fibra óptica Mono Modo (SMF) 10 Gb	10
	2	Módulo SFP para fibra óptica Multi Modo (MMF) 10 Gb	8
	3	Módulo SFP para fibra óptica Multi Modo (MMF) 1 Gb	6

## De las MIPYMES

Para los procedimientos de Menor Cuantía, este tipo de procedimiento de contratación estará preferentemente reservado a las MIPYMES, de conformidad al artículo 34 inc b) de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas". Son consideradas Mipymes las unidades económicas que, según la dimensión en que organicen el trabajo y el capital, se encuentren dentro de las categorías establecidas en el Artículo 5° de la Ley N° 4457/2012 "PARA LAS MICRO, PEQUEÑAS Y MEDIANAS EMPRESAS", y se ocupen del trabajo artesanal, industrial, agroindustrial, agropecuario, forestal, comercial o de servicio

## Plan de entrega de los bienes

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

Lote	Ítem	Descripción	Cantidad	Dependencia	Lugar Entrega	Fecha entrega
1	1	Servidor para clúster	3	DS	Departamento de Informática - CRA - DGAF, con	Deberán ser entregados en su totalidad en un plazo no superior a 60 días calendario contados desde la recepción de la orden de compra.
2	1	Sistema de Almacenamiento - Storage	1		acompañamiento del Departamento de Aprovevisionamiento -CRA - DGAF	
3	Equipos de comunicación					Deberán ser entregados en su totalidad en un plazo no superior a 60 días calendario contados desde la recepción de la orden de compra.
	1	Firewall de Borde	1			
	2	Punto de Acceso - WIFI	30			

3	Cliente VPN y solución de seguridad para estaciones de trabajo	500	
4	Analizador de tráfico y Seguridad	1	
4	Módulos SFP		Deberán ser entregados en su totalidad en un plazo no superior a 30 días calendario contados desde la recepción de la orden de compra.
1	Módulo SFP para fibra óptica Mono Modo (SMF) 10 Gb	10	
2	Módulo SFP para fibra óptica Multi Modo (MMF) 10 Gb	8	
3	Módulo SFP para fibra óptica Multi Modo (MMF) 1 Gb	6	

## Planos y diseños

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

No Aplica

## Embalajes y documentos

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

No Aplica



## Inspecciones y pruebas

Las inspecciones y pruebas serán como se indica a continuación:

Durante la implementación serán realizadas las pruebas de los equipos en un ambiente controlado conjuntamente con técnicos del MEF de acuerdo a las configuraciones necesarias que serán documentadas. Al finalizar la implementación se deberá entregar un informe del proceso.

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

## Indicadores de Cumplimiento

El documento requerido para acreditar el cumplimiento contractual, será:

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA (se indica la fecha que debe presentar según el PBC)
-----------	------	--

Conformidad de la recepción del bien por parte del Departamento de Informática.	Informe de conformidad / Nota de remisión	El ítem 1 del lote 1, ítem 1 del lote 2, los ítems 1, 2, 3, 4 del lote 3 deberán ser entregados dentro de los 60 días calendario contados desde la recepción de la orden de compra
Conformidad de la recepción del bien por parte del Departamento de Informática.	Informe de conformidad / Nota de remisión	Los ítems 1, 2, 3 del lote 4 deberán ser entregados dentro de los 30 días calendario contados desde la recepción de la orden de compra

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

# CONDICIONES CONTRACTUALES

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

## Interpretación

1. Si el contexto así lo requiere, el singular significa el plural y viceversa; y "día" significa día calendario, salvo que se haya indicado expresamente que se trata de días hábiles.
2. Condiciones prohibidas, inválidas o inejecutables. Si cualquier provisión o condición del contrato es prohibida o resultase inválida o inejecutable, dicha prohibición, invalidez o falta de ejecución no afectará la validez o el cumplimiento de las otras provisiones o condiciones del contrato.
3. Limitación de Dispensas:
  - a) Toda dispensa a los derechos o facultades de una de las partes en virtud del contrato, deberá ser documentada por escrito, indicar la fecha, estar firmada por un representante autorizado de la parte que otorga dicha dispensa, deberá especificar la obligación dispensada y el alcance de la dispensa.
  - b) Sujeto a lo indicado en el inciso precedente, ningún retraso, prórroga, demora o aprobación por cualquiera de las partes al hacer cumplir algún término y condición del contrato o el otorgar prórrogas por una de las partes a la otra, perjudicará, afectará o limitará los derechos de esa parte en virtud del contrato. Asimismo, ninguna prórroga concedida por cualquiera de las partes por un incumplimiento del contrato, servirá de dispensa para incumplimientos posteriores o continuos del contrato.

## Formalización de la contratación

Se formalizará esta contratación mediante:

Contrato

## Documentación requerida para la firma del contrato

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

### 1. Personas Físicas / Jurídicas

- Certificado de no encontrarse en quiebra o en convocatoria de acreedores expedido por la Dirección General de Registros Públicos;
- Certificado de no hallarse en interdicción judicial expedido por la Dirección General de Registros Públicos; Constancia de no adeudar aporte obrero patronal expedida por el Instituto de Previsión Social.
- Certificado laboral vigente expedido por la Dirección de Obrero Patronal dependiente del Viceministerio de Trabajo, siempre que el sujeto esté obligado a contar con el mismo, de conformidad a la reglamentación pertinente - CPS
- En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para

- asumir todas las obligaciones emergentes del contrato hasta su terminación.
- Certificado de cumplimiento tributario vigente a la firma del contrato.

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

## 2. Documentos. Consorcios

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

La convocante deberá requerir la presentación de los certificados, de conformidad al numeral 1.1, al oferente que resultare adjudicado, con anterioridad a la firma del contrato. Si el oferente no presentare dichos certificados o realizare una declaración jurada falsa, la adjudicación será revocada, la garantía de mantenimiento de oferta será ejecutada y los antecedentes serán remitidos a la Dirección Nacional de Contrataciones Públicas.

## Subcontratación

El porcentaje permitido para la subcontratación será de:

No Aplica

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

## Derechos Intelectuales

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

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

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

Dicha indemnización no procederá si los bienes o una parte de ellos fuesen utilizados para fines no previstos en el contrato o para fines que no pudieran inferirse razonablemente del contrato. La indemnización tampoco cubrirá cualquier transgresión que resultará del uso de los bienes o parte de ellos, o de cualquier producto producido como resultado de asociación o

combinación con otro equipo, planta o materiales no suministrados por el proveedor en virtud del contrato.

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

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

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

6. La contratante deberá indemnizar y eximir de culpa al proveedor y a sus empleados, funcionarios y subcontratistas, por cualquier litigio, acción legal o procedimiento administrativo, reclamo, demanda, pérdida, daño, costo y gasto, de cualquier naturaleza, incluyendo honorarios y gastos de abogado, que pudieran afectar al proveedor como resultado de cualquier transgresión o supuesta transgresión de patentes, modelos de aparatos, diseños registrados, marcas registradas, derechos de autor, o cualquier otro derecho de propiedad intelectual registrado o ya existente a la fecha del contrato, que pudieran suscitarse con motivo de cualquier diseño, datos, planos, especificaciones, u otros documentos o materiales que hubieran sido suministrados o diseñados por la contratante o a nombre suyo.

## Transporte

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

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

No Aplica

## Confidencialidad de la información

1. No deberá darse a conocer información alguna acerca del análisis, aclaración y evaluación de las ofertas, mientras dure el mismo de conformidad con el artículo N° 52 de la Ley N° 7021/22 “De Suministro y Contrataciones Públicas”, ni sobre las recomendaciones relativas a la adjudicación, después de la apertura en público de las ofertas, a los oferentes ni a personas no involucradas en el proceso de evaluación, hasta que haya sido dictada la resolución de adjudicación cuando se trate de un solo sobre. En las respuestas a las solicitudes de aclaración, los oferentes deberán indicar si la información suministrada es de carácter reservado, debiendo precisar la norma legal que la establece como secreta o de carácter reservado, de conformidad a lo estipulado en la Ley N° 5282/14 “DE LIBRE ACCESO CIUDADANO A LA INFORMACIÓN PÚBLICA Y TRANSPARENCIA GUBERNAMENTAL”. Cuando se trate de dos sobres, la confidencialidad de la primera etapa será hasta la emisión del acto administrativo de selección de ofertas técnicas, reanudándose la confidencialidad después de la apertura en público de las ofertas económicas hasta la emisión de la resolución de adjudicación.

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

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

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

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

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

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

## **Obligatoriedad de declarar información del personal del proveedor o contratista en el SICP**

1. El proveedor deberá proporcionar los datos de identificación de sus subproveedores, así como de las personas físicas por medio de las cuales propone cumplir con las obligaciones del contrato, dentro de los treinta días posteriores a la obtención del código de contratación, y con anterioridad al primer pago que vaya a percibir en el marco de dicho contrato, con las especificaciones respecto a cada una de ellas. A ese respecto, el contratista deberá consignar dichos datos en el Formulario de Identificación del Personal (FIP) y en el Formulario de Identificación de Servicios Personales (FIS), a través del Registro del Proveedor del Estado.

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

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

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

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

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

## **Porcentaje de Garantía de Fiel Cumplimiento de Contrato**

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

10,00 %

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

---

## **Forma de Instrumentación de Garantía de Fiel Cumplimiento de Contrato**

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

---

## **Periodo de validez de la Garantía de Cumplimiento de Contrato**

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

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

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

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

---

## **Formas y condiciones de pago**

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

### **1. Documentos Genéricos:**

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

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

### **CONDICIONES DE PAGO:**

El PROVEEDOR presentará la solicitud de pago a través de la Dirección General de Administración y Finanzas por escrito y adjuntará a dicha solicitud: Nota de solicitud de pago; Nota de Remisión y Acta de Recepción respecto de los bienes que fueron entregados a entera satisfacción de la contratante, con la conformidad de los administradores del contrato y/o los responsables designados para el efecto, debiendo contar con el V°B° de la Coordinación de Recursos Administrativos;

La factura con timbrado vigente, la cual deberán expresar claramente por separado el Impuesto al Valor Agregado (IVA) de

conformidad con las disposiciones tributarias aplicables, asimismo deberán estar debidamente llenadas con los siguientes datos: Ministerio de Economía y Finanzas R.U.C.80024627-6, descripción del servicio, número de contrato, número de orden de compra/servicio, modalidad del contrato. En ningún caso el valor total facturado podrá exceder el valor adjudicado o las adendas aprobadas;

Orden de Compra/ Servicio REPSE (Registro de Prestadores de Servicios) todos los que son prestadores de servicios;

Certificado de Cumplimiento Tributario;

Constancia de Cumplimiento con la Seguridad Social;

Formulario de informe de servicios personales (FIS); y

Formulario de Identificación de Personal(FIP).

En caso de facturas emitidas a través de sistemas informáticos de pre impresión de facturas, que no permitan la consignación de dichos datos, los mismos podrán ser completados en el reverso de la factura precedidas de la inscripción Léase. Del monto total facturado, serán pasibles las retenciones correspondientes al Impuesto a la Renta y al Impuesto al Valor Agregado, según lo establecido por las disposiciones legales de la República del Paraguay. Asimismo, independientemente de estas retenciones impositivas, se aplicará una Retención sobre el monto de las facturas pagadas, deducidos los impuestos reflejados en las mismas en concepto de Contribución de conformidad a lo dispuesto en la Ley 7021/22 De Suministro y Contrataciones Públicas, y conforme lo dispone la reglamentación vigente. -

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

3. De conformidad a las disposiciones del Decreto N° 7781/2006, del 30 de Junio de 2006 y modificatoria, en las contrataciones con Organismos de la Administración Central, el proveedor deberá habilitar su respectiva cuenta corriente o caja de ahorro en un Banco de plaza y comunicar a la Contratante para que ésta gestione ante la Dirección General del Tesoro Público, la habilitación en el Sistema de Tesorería (SITE).

## **Solicitud de suspensión de la ejecución del contrato**

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

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

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

## **Anticipo MIPYMES**

Se otorgará Anticipo MIPYMES:

No Aplica



---

## **Solicitud de Pago de Anticipo**

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

No Aplica

---

## **Forma de Instrumentación de Garantía de anticipo**

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

No Aplica

---

## **Reajuste**

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

El precio del contrato estará sujeto a reajustes. La fórmula y el procedimiento para el reajuste serán los siguientes: Siempre y cuando la variación del IPC publicado por el BCP haya sufrido una variación igual o mayor al quince por ciento (15%) referente a la fecha de apertura de ofertas:

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

IPC0

Dónde:

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

IPC0: Índice de precios al consumidor publicado por el Banco Central de Paraguay, correspondiente al mes de la apertura de sobres.

El reajuste será aplicado a aquella parte del servicio pendiente de ejecución luego de la variación de precios. No se reconocerán reajustes de precios si el suministro se encuentra atrasado respecto al cronograma de prestación de servicios.

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

---

## **Porcentaje de multas**

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

0,50 %

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

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

## **Tasa de interés por Mora**

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

0,01

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

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

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

## **Impuestos y derechos**

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

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

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

No Aplica

## **Convenios Modificatorios**

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

1. Cuando el sistema de adjudicación adoptado sea de abastecimiento simultáneo las ampliaciones de los contratos se registrarán por las disposiciones contenidas en la Ley N° 7021/22, sus modificaciones y reglamentaciones, que para el efecto emita la

DNCP.

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

## Limitación de responsabilidad

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

## Responsabilidad del proveedor

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

## Fuerza mayor

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

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

A menos que la contratante disponga otra cosa por escrito, el proveedor continuará cumpliendo con sus obligaciones en virtud

del contrato en la medida que sea razonablemente práctico, y buscará todos los medios alternativos de cumplimiento que no estuviesen afectados por la situación de fuerza mayor existente.

## **Causales de terminación del contrato**

### **1. Terminación por Incumplimiento**

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

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

### **2. Terminación por insolvencia o quiebra**

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

### **3. Terminación por conveniencia**

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

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

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

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

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

## **Otras causales de terminación del contrato**

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

Los descriptos en la Ley 7021/22 de "SUMINISTROS Y CONTRATACIONES PÚBLICAS".

## Fraude y Corrupción

1. La convocante exige que los participantes en los procedimientos de contratación, observen los más altos niveles éticos, ya sea durante el proceso de licitación o de ejecución de un contrato. La convocante actuará frente a cualquier hecho o reclamación que se considere fraudulento o corrupto.
2. Si se comprueba que un funcionario público, o quien actúe en su lugar, y/o el oferente o adjudicatario propuesto en un proceso de contratación, hayan incurrido en prácticas fraudulentas o corruptas, la convocante deberá:
  - (i) En la etapa de oferta, se descalificará cualquier oferta del oferente y/o rechazará cualquier propuesta de adjudicación relacionada con el proceso de adquisición o contratación de que se trate; y/o
  - (ii) Durante la ejecución del contrato, se rescindirá el contrato por causa imputable al proveedor;
  - (iii) Se remitirán los antecedentes del oferente o proveedor directamente involucrado en las prácticas fraudulentas o corruptivas, a la Dirección Nacional de Contrataciones Públicas, a los efectos de la aplicación de las sanciones previstas.
  - (iv) Se presentará la denuncia ante las instancias correspondientes si el hecho conocido se encontrare tipificado en la legislación penal.

Fraude y corrupción comprenden actos como:

- (i) Ofrecer, dar, recibir o solicitar, directa o indirectamente, cualquier cosa de valor para influenciar las acciones de otra parte;
  - (ii) Cualquier acto u omisión, incluyendo la tergiversación de hechos y circunstancias, que engañen, o intenten engañar, a alguna parte para obtener un beneficio económico o de otra naturaleza o para evadir una obligación;
  - (iii) Perjudicar o causar daño, o amenazar con perjudicar o causar daño, directa o indirectamente, a cualquier parte o a sus bienes para influenciar las acciones de una parte;
  - (iv) Colusión o acuerdo entre dos o más partes realizado con la intención de alcanzar un propósito inapropiado, incluyendo influenciar en forma inapropiada las acciones de otra parte.
  - (v) Cualquier otro acto considerado como tal en la legislación vigente.
3. Los oferentes deberán declarar que por sí mismos o a través de interpósita persona, se abstendrán de adoptar conductas orientadas a que los funcionarios o empleados de la convocante induzcan o alteren las evaluaciones de las propuestas, el resultado del procedimiento u otros aspectos que les otorguen condiciones más ventajosas con relación a los demás participantes.

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

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

## Medio Alternativo de Resolución de Conflictos a través de la Mediación

El procedimiento de Mediación se podrá llevar a cabo ante:

- El Centro de Arbitraje y Mediación del Paraguay.

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

Todas las controversias que deriven del presente contrato o que guarden relación con éste y sean susceptibles de transacción o conciliación, podrán ser resueltas por mediación, conforme con las disposiciones de la Ley N° 7021/22 “De Suministro y Contrataciones Públicas”, de la Ley N° 1879/02 “De Arbitraje y Mediación” y las condiciones del contrato. El proceso será presidido mediante la asistencia de un tercero neutral, denominado mediador, de conformidad a la sede establecida. Se aplicará el reglamento respectivo y demás disposiciones que regulen 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 acta de Mediación, 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.

---

**Medio alternativo de Resolución de Conflictos a través del Arbitraje**

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

No Aplica

# MODELO DE CONTRATO

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

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

# FORMULARIOS

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

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



