REPÚBLICA DEL PARAGUAY

PLIEGO DE BASES Y CONDICIONES

Convocante:

Administración Nacional de Navegación y Puertos (ANNP)

Uoc Annp

Nombre de la Licitación:

ADQUISICION E INSTALACION DE EQUIPOS DE SEGURIDAD FIREWALL - LLAVE EN MANO

(versión 2)

ID de Licitación:

485938

Modalidad:

Licitación Pública Nacional

Publicado el:

18/09/2026

"Pliego para la Adquisición de Bienes y/o Servicios - CONVENCIONAL - Ley Nº 7021/22."
Versión 4

RESUMEN DEL LLAMADO

Datos de la Convocatoria

ID de Licitación:	485938	**Nombre de la Licitación:**	ADQUISICION E INSTALACION DE EQUIPOS DE SEGURIDAD FIREWALL - llave en mano
Convocante:	Administración Nacional de Navegación y Puertos (ANNP)	**Categoría:**	43000000 - Tecnologias de Informacion, Telecomunicaciones y Radiodifusiones
Unidad de Contratación:	Uoc Annp	**Tipo de Procedimiento:**	LPN - Licitación Pública Nacional

Etapas y Plazos

Lugar para Realizar Consultas:	en SICP	**Fecha Límite de Consultas:**	23/09/2026 12:00
Lugar de Entrega de Ofertas:	MESA DE ENTRADA DE LA UOC- El Paraguayo Independiente y Colon - Primer Piso	**Fecha de Entrega de Ofertas:**	30/09/2026 08:20
Lugar de Apertura de Ofertas:	OFICINA DE LA GERENCIA DE LA UOC- El Paraguayo Independiente y Colon - Primer Piso	**Fecha de Apertura de Ofertas:**	30/09/2026 08:30

Adjudicación y Contrato

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

Datos del Contacto

Nombre:	CARLOS MARTIN FIGUEREDO	**Cargo:**	GERENTE DE UOC
Teléfono:	0214392161	**Correo Electrónico:**	uocannp@gmail.com

ADENDA

Adenda

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

ADENDA N° 1

Señores oferentes

La ANNP ha emitido la siguiente la adenda en la cual se modifica las Especicificaciones tecnicas y se prorrogan los plazos para la presentacion y apertura de sobres de oferta.

Atte.

Se detectaron modificaciones en las siguientes cláusulas:

Sección: Suministros requeridos - especificaciones técnicas

- Detalle de los bienes y/o servicios

Se puede realizar una comparación de esta versión del pliego con la versión anterior en el siguiente enlace: https://www.contrataciones.gov.py/licitaciones/convocatoria/1f179633-a9cc-6782-abfd-4f6aba28f48f/pliego/2/diferencias/1.html?seccion=adenda

La adenda es el documento emitido por la convocante, mediante la cual se modifican aspectos establecidos en las bases de la contratación. A los efectos legales, la adenda será considerada parte integrante del documento cuyo contenido modifique.

La convocante podrá introducir modificaciones cuando se ajuste a los parámetros establecidos en la Ley.

Las adendas serán difundidas en el SICP respetando los plazos establecidos en la resolución por la cual se Reglamentan los Procedimientos de Contratación regidos por la Ley N° 7021/22.

Obs: Cuando la convocante requiera prorrogar la fecha tope de presentación y apertura de ofertas, sin modificar los demás datos e información de las bases de la contratación, será difundida automáticamente a través del SICP y no se instrumentará a traves de adenda.

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 Sostenible - CPS

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

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

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

Criterios sociales y económicos:

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

Criterios ambientales:

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

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

Conducta empresarial responsable:

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

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

Aclaración de los documentos de la convocatoria

1. Consultas electrónicas.

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

2. Respuestas y aclaraciones.

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

3. Adendas y prórrogas del tope para consultas.

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

4. Emisión de aclaraciones sobre Adendas.

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

5. Junta de aclaraciones.

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

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

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

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.

5. Cuando la Garantía de Mantenimiento de Ofertas sea instrumentada a través de Declaración Jurada, deberá estar firmada en todas sus páginas.

Plazo para presentar las ofertas

Las ofertas deberán ser presentadas 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 prevista.

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. La inscripción en el Registro de Proveedores del Estado por parte de todos los miembros del consorcio, constituye requisito previo para la presentación de las ofertas, los cuales deberán encontrarse activos en el Registro. Se deberá realizar el procedimiento de activación del consorcio directamente a través del Registro de Proveedores.

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

Los integrantes de un consorcio no podrán presentar ofertas individuales ni conformar más de un consorcio para un mismo lote o ítem, lo que no impide que puedan presentarse en diferentes partidas de manera individual o como miembro de otro consorcio.

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

Idioma de la oferta

La oferta deberá ser presentada en idioma castellano.

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

No Aplica

Cuando se admitiera la presentación de anexos técnicos y folletos en idioma distinto al español, su traducción deberá ser realizada por un traductor público matriculado en la República del Paraguay.

Lista de Precios

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 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.

e) En todos los casos, independientemente al sistema de adjudicación, el oferente deberá indicar el CPEN respectivo al ítem ofertado, en caso de contar. Dicho atributo tendrá carácter formal siendo susceptible de aclaraciones por parte del comité de evaluación.

2. Los precios indicados en la lista de precios serán consignados separadamente, de acuerdo a lo previsto en el SICP y según se detalla a continuación:

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 multiplicando los precios unitarios por la cantidad máxima correspondiente.

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

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

6. 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 este apartado se deberá indicar la manera de distribución de los mismos:

No Aplica

Supuesto de abastecimiento simultáneo

El abastecimiento se regirá por el supuesto de:

No Aplica

Moneda de la oferta y pago

La moneda de la oferta y pago será:

Moneda Nacional

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

Moneda extranjera

La moneda extranjera para la oferta y pago, será:

No Aplica

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:

Ninguna Copia

Documentos de la oferta

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

1. **Constancia del Perfil del proveedor.**
    1. 1.**Ofertas físicas**

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

Será considerada válida la Constancia que se presente con firma manuscrita o electrónica cualificada por él o los representantes legales.

1.2.**Ofertas electrónicas**

Cuando la presentación de oferta sea electrónica, no se admitirá la presentación de la constancia de perfil del proveedor. El proveedor deberá proceder a la vinculación de los documentos del Registro de Proveedores del Estado a través del Módulo de Ofertas Electrónicas, según lo dispuesto en las disposiciones vigentes.

2. **Confidencialidad de documentos.**

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

Ofertas Alternativas

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

No Aplica

Una oferta alternativa se configura necesariamente con la presentación de la oferta principal, que se ajuste a las condiciones previstas en las bases y condiciones; y, de manera separada e independiente una propuesta alternativa, que implique alternativas técnicas a los requerimientos de la licitación y cuya consideración estaría sujeta a que dicha alternativa reúna mejores condiciones de oportunidad, calidad y costo.

Periodo de validez de las ofertas

Las ofertas deberán mantenerse válidas por:

90

días corridos.

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

La convocante, en circunstancias excepcionales, podrá solicitar por escrito a los oferentes la extensión del periodo de validez de la oferta. En caso de aceptar dicha solicitud, el oferente deberá manifestar su consentimiento de forma expresa, y, en consecuencia, prorrogar igualmente la Garantía de Mantenimiento de la Oferta.

El oferente podrá rechazar la solicitud de prórroga sin que ello implique la ejecución de su Garantía de Mantenimiento de la Oferta. En caso de aceptar la extensión solicitada, no se le pedirá ni se le permitirá modificar su oferta.

Garantías: instrumentación, plazos y ejecución.

1. Instrumentación y porcentaje

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

a. Garantía bancaria emitida por un banco establecido en la República del Paraguay, la que deberá ajustarse a las condiciones establecidas por la DNCP.
b. Póliza de seguros emitida por una compañía autorizada a operar y emitir pólizas de seguros de caución en la República del Paraguay. La póliza deberá ajustarse a las condiciones establecidas por la DNCP.
c. En los procedimientos, cuyo monto de estimación de la contratación sea inferior a los dos mil (2.000) jornales mínimos, se admitirá la instrumentación de las garantías de mantenimiento de ofertas a través de Declaraciones Juradas con certificación de firma por Escribano Público. La certificación de firma podrá corresponder a la misma fecha del documento certificado o a una fecha posterior, siempre y cuando sea de fecha previa a la presentación y apertura de sobres.
d. En caso de utilizarse el Módulo de Ofertas Electrónicas, las declaraciones juradas serán generadas y firmadas a través del módulo y no requerirán certificación de firmas.

1. 2. En los contratos abiertos, el porcentaje de las garantías a ser presentado por los oferentes que participen, deberá ser aplicado sobre el monto máximo total del llamado; si la adjudicación fuese por lote o ítem ofertado, deberán sumarse los valores máximos de cada lote o ítem ofertado, o de la suma de los valores máximos obtenidos por la multiplicación de los precios unitarios ofertados con las cantidades máximas, a fin de obtener el monto sobre el cual se aplicará el porcentaje de la citada garantía.

1. 3. En caso de instrumentarse las garantías a través de Garantía Bancaria o Declaración jurada, deberá estar sustancialmente de acuerdo con el formulario incluido en la Sección "Formularios".

2. Garantía de mantenimiento de ofertas en consorcios

2.1.En caso de consorcios, la garantía de mantenimiento de ofertas deberá ser presentada de la siguiente manera:

a. Consorcio constituido por escritura pública: deberán emitir a nombre del consorcio legalmente constituido por escritura pública o del gestor y representante del consorcio (Empresa líder), designado en la escritura pública.
b. Consorcio con acuerdo de intención de participación en contrato de consorcio: deberán emitir a nombre del gestor y representante del consorcio (empresa líder), designado en el acuerdo.

3. Ejecución de la Garantía de mantenimiento de ofertas

3.1. La Garantía de Mantenimiento de Ofertas podrá ser ejecutada:

a. 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,

e. Cuando se comprobare que las declaraciones juradas presentadas por el oferente adjudicado con su oferta sean falsas,

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

g. Si el adjudicatario no presentare las legalizaciones correspondientes para la firma del contrato, cuando éstas sean requeridas.

La Garantía de Mantenimiento de Oferta, sea cual fuere la forma de instrumentación adoptada, cuando se tenga acreditada una de las causales de ejecución de la garantía deberá ser pagadera según el tipo de garantía que haya sido solicitada.

Periodo de Validez de la Garantía de Mantenimiento de Oferta

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

120

días corridos.

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

El plazo mínimo de validez será de al menos 30 días posteriores al plazo de validez establecido para las ofertas.

Condiciones especiales de la Garantía de Mantenimiento de Oferta

Las condiciones especiales de la Garantía de Mantenimiento de Oferta serán:

No Aplica

Subcontratación

El porcentaje permitido para la subcontratación será de:

No Aplica

El oferente podrá indicar junto con la oferta las personas a ser subcontratadas, o, en la etapa contractual previa a la autorización por parte de la contratante. El formulario de personas a subcontratar/subcontratadas, deberá ser presentado de acuerdo a la etapa en la que se indique la subcontratación, siendo susceptible de evaluación respecto a las inhabilidades del Art 21 de la Ley N° 7021/22.

Método de presentación 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, RUC 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.

Para los casos de consorcios con acuerdo de intención, los sobres deberán contemplar el RUC provisorio generado en el Registro de Proveedores.

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.

En caso de la utilización del módulo de ofertas electrónicas, la misma se regirá por las disposiciones establecidas en la normativa vigente y la guía de ofertas electrónicas.

Cuando el sobre no cuente con el RUC, se podrá subsanar dicha omisión al momento de la presentación.

Retiro, sustitución y modificación de las ofertas

1. Ofertas físicas.

1.1 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.

1.2. 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) Realizadas antes del plazo límite establecido para el acto de apertura de ofertas cuando las ofertas sean identificadas con “RETIRO”, y;

c) Realizadas antes del plazo límite establecido para la presentación de ofertas cuando las ofertas sean identificadas con “SUSTITUCIÓN” o “MODIFICACIÓN”.

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

1.3. Ninguna oferta podrá ser retirada durante el intervalo comprendido entre la fecha límite para el acto de apertura 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.

1.4. Ninguna oferta podrá ser 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.

2. Ofertas electrónicas.

2.1. Un oferente podrá retirar, sustituir o modificar su oferta después de presentada, hasta antes de la fecha límite de presentación y apertura de ofertas, para ello deberá sujetarse a la reglamentación pertinente.

Apertura de ofertas

1. Desarrollo del acto de apertura de ofertas.

1.1. La entidad convocante procederá a la apertura de las ofertas en acto público en presencia de los oferentes o sus representantes según la hora, fecha y lugar previamente establecidos en el SICP.

1.2. 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.

1.3. Primero la convocante deberá verificar que los oferentes se encuentren inscriptos en el Registro de Proveedores del Estado conforme con los datos previstos en el sobre, en caso de que, no sea posible identificar al oferente mediante el sobre presentado, la UOC procederá a abrirlo con el fin de verificar el número de RUC incluido entre los documentos de la oferta, para constatar si el oferente se encuentra inscripto en el Registro de Proveedores del Estado. En caso de que el oferente no inscripto en el Registro haya presentado la oferta, la convocante deberá dejar constancia en el acta de apertura electrónica.

La oferta del oferente no inscripto que cuente con la identificación de RUC en el sobre, no será abierta sino devuelto al oferente remitente. La oferta del oferente que no cuente con la identificación de RUC en el sobre será abierta y remitida al órgano evaluador de la convocante, para la evaluación de la oferta o su rechazo, según corresponda.

La presente disposición será aplicable en los procedimientos de doble sobre en los que será abierta la oferta técnica para la verificación respectiva, siempre y cuando la misma esté debidamente identificada como sobre técnico.

Esta disposición no será aplicable a los procedimientos que utilicen el módulo de ofertas electrónicas y a aquellos procedimientos especiales que, por su naturaleza, expresamente no requieran de la inscripción en el Registro de Proveedores del Estado como condición de participación.

1.4. Luego 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.

1.5. 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.

1.6. 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. El acta se difundirá a través del SICP.

1.7. 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.

1.8. Si los sobres no están cerrados e identificados como se requiere, la convocante deberá dejar constancia de ello en el acto de apertura y no se responsabilizará en caso de que la oferta se extravíe o sea abierta prematuramente.

1.9. 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.

2. Comunicación del acta de apertura.

2.1. 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.

2.2. 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

1. **Difusión de la visita.**

La visita o inspección técnica deberá fijarse de forma previa a la fecha tope de consulta, previendo como mínimo el plazo de difusión de (02) dos días hábiles. En todos los casos, el procedimiento para su realización deberá difundirse en las bases de la contratación.

Cuando la convocante haya establecido la visita o inspección técnica, en las bases de la contratación, el oferente que conozca el sitio podrá declarar bajo fe de juramento conocer el sitio y que cuenta con la información suficiente para preparar la oferta y ejecutar el contrato.

Cuando por la naturaleza o complejidad de la contratación sea imprescindible la realización de la visita técnica, la convocante podrá establecer la obligatoriedad de dicha visita a través del SICP. En estos casos no se aceptará la presentación de la declaración jurada.

2. **Desarrollo de la visita.**

Se registrará en acta los asistentes, la fecha, lugar, hora de realización y funcionarios participantes. Los representantes de los oferentes que asistan a la visita podrán contar con una autorización, bastando para ello la presentación de una nota del oferente. La falta de presentación de esta autorización no impide su participación en la visita o inspección técnica.

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

Incoterms

La edición de incoterms para esta licitación será:

No Aplica

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

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

Autorización del Fabricante

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

EL OFERENTE DEBERA PRESENTAR LA CARTA DE AUTORIZACION DEL FABRICANTE DE LOS EQUIPOS OFERTADOS EN EL PRESENTE LLAMADO. (LA NOTA DEL FABRICANTE DEBERA ESTAR DIRIGIDA A LA INSTITUCION Y CON REFERENCIA AL PROCESO DE LICITACION. NO SE ACEPTARAN CARTAS GENERICAS)

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 serán consideradas requisito indispensable para la evaluación de la oferta. Las mismas deberán ser presentadas en el momento determinado en este apartado. La falta de presentación de las muestras en tiempo y condiciones establecido por la Convocante será causal de descalificación de la oferta.

Tiempo de funcionamiento de los bienes

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

No Aplica

Plazo de reposición de bienes

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

2 DIAS HABILES

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:

SE REQUERIRA UNA GARANTIA DEL FABRICANTE POR EL TERMINO DE 3 AÑOS, CONTADOS A PARTIR DE LA ENTREGA TOTAL DE LOS EQUIPOS , CONFORME LO REQUERIDO EN LAS ESPECIFICACIONES TECNICAS.

Cobertura de Seguro de los bienes

La cobertura de seguro requerida a los bienes será:

No Aplica

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

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.

Confidencialidad de la Información

Reserva de información en respuestas a aclaraciones.

En las respuestas a las solicitudes de aclaración, los oferentes deberán indicar si la información suministrada es de carácter reservado, debiendo precisar la norma legal que la establece como secreta o de carácter reservado, de conformidad a lo estipulado en la Ley N° 5282/14 ‘’DE LIBRE ACCESO CIUDADANO A LA INFORMACIÓN PÚBLICA Y TRANSPARENCIA GUBERNAMENTAL’’.

REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN

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

Condición de Participación

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

Los oferentes domiciliados en la República del Paraguay, que pretendan participar en un procedimiento de contratación, no deberán estar comprendidos en las prohibiciones o limitaciones para presentar propuestas y contratar con el Estado, establecidas en el artículo 21 de la Ley N° 7021/22 "DE SUMINISTROS Y CONTRATACIONES PUBLICAS".

Sucursales

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

Conflicto de Interés

1. Deber de Abstención del funcionario ante un posible conflicto de interés. El funcionario público que participe en el procedimiento de contratación deberá abstenerse de intervenir, de manera directa o indirecta, en los asuntos en los que su actuación esté comprendida en alguno de los supuestos del artículo 17 de la Ley N° 7021/22. A tales efectos, deberá comunicar a su superior jerárquico o a la máxima autoridad institucional que se encuentra inmerso en uno de los supuestos legales, detallando la situación particular. En caso que corresponda, el superior jerárquico o la máxima autoridad institucional tendrá por aceptada la abstención apartando al funcionario y, de ser necesario, designará al sustituto. Se deberá dejar constancia por escrito de todo lo actuado.

2. Apartamiento del funcionario por la Entidad Convocante. Enterada la Convocante de que existe un conflicto de interés respecto a un funcionario público que ha sido designado o requerido para intervenir o que interviene en alguna de las etapas de la fase de contratación del suministro público, y no mediando la abstención expresa del funcionario, deberá apartarlo del asunto particular, detallando la situación que configura el conflicto de interés. La Convocante deberá dejar constancia por escrito de todo lo actuado. Se procederá a la designación del sustituto, en los casos que correspondiere.

3. Actuaciones tras la detección de un conflicto de interés. Si la Entidad Convocante detectare que un funcionario público comprendido en alguno de los supuestos del artículo 17 de la Ley N° 7021/22 tuvo intervención en alguna de las etapas de la fase de contratación del suministro público, adoptará las medidas que correspondan. La Convocante podrá subsanar las actuaciones en sede administrativa o revocarlas, según corresponda. Deberá dejarse constancia por escrito de todo lo

actuado y comunicarse a la DNCP. La DNCP podrá, de oficio o por denuncia fundada, realizar las investigaciones que resulten pertinentes, a fin de verificar presuntos hechos que podrían constituir conflicto de intereses y/o irregularidades en contravención con el artículo 17 de la Ley N° 7021/22, conforme las atribuciones conferidas en el artículo 132 de la Ley.

4. Declaración jurada de conocimiento de la existencia de un conflicto de intereses respecto a los funcionarios públicos intervinientes en el procedimiento. La convocante deberá verificar la "Declaración jurada de conocimiento de la existencia de un conflicto de intereses respecto a los funcionarios públicos intervinientes en el procedimiento" presentada por el oferente al momento de la oferta en cumplimiento de su obligación de comunicar o denunciar la existencia de posibles conflictos de intereses, de conformidad al artículo 17 de la Ley 7021/22. De comprobarse la omisión, falsedad o inexactitud de la información proporcionada y declarada en la Declaración la Convocante analizará si se configura un conflicto de interés en los términos del artículo 17 de la Ley 7021/22 y emitirá las directrices que correspondan acorde a la etapa del procedimiento de contratación. Además, la Convocante podrá resolver la descalificación de la oferta y/o rescisión del contrato respectivo.

Confidencialidad de la etapa de evaluación de ofertas.

No deberá darse a conocer información alguna acerca del análisis, aclaración y evaluación de las ofertas, mientras dure el mismo de conformidad con el artículo N° 52 de la Ley N° 7021/22 ''De Suministro y Contrataciones Públicas'', ni sobre las recomendaciones relativas a la adjudicación, después de la apertura en público de las ofertas, a los oferentes ni a personas no involucradas en el proceso de evaluación, hasta que haya sido dictada la resolución de adjudicación cuando se trate de un solo sobre. Cuando se trate de dos sobres, la confidencialidad de la primera etapa será hasta la emisión del acto administrativo de selección de ofertas técnicas, reanudándose la confidencialidad después de la apertura en público de las ofertas económicas hasta la emisión de la resolución de adjudicación.

Requisitos de Calificación

Calificación Legal. Los oferentes deberán declarar que no se encuentran comprendidos en las limitaciones o prohibiciones para contratar con el Estado, según lo establecido en el artículo 21 de la Ley Nº 7021/22. Esta declaración forma parte del formulario de oferta.

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

A los efectos de la verificación de la existencia de prohibiciones o limitaciones contenidas en el artículo 21 de la Ley Nº 7021/22, el comité de evaluación realizará el siguiente análisis:

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

2º Además, deberá verificar la presentación de la declaración jurada de conocimiento de la existencia de un conflicto de intereses respecto a los funcionarios públicos intervinientes en el procedimiento, y de las constancias de registro de estructura jurídica y de beneficiarios finales, a fin de verificar que los oferentes no se encuentren incursos en las causales previstas en los Arts. 17 y 21 de la Ley Nº 7021/22.

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

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

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

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

7º El comité verificará en fuentes públicas de información de libre acceso, si el oferente o sus integrantes, se encuentran en los demás supuestos contenidos en el artículo 21 de la Ley Nº 7021/22, pudiendo utilizar como guía instructiva el documento aprobado por la DNCP. En caso de requerirse, el comité podrá solicitar aclaración al oferente sobre la vigencia de la información obrante en las fuentes respectivas.

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

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

Método de Evaluación

Basado únicamente en precio

En caso de optar por el método de multiplicidad de criterios deberá estar supeditado a los lineamientos emitidos por el MEF y la DNCP.

Análisis de precios ofertados

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

Luego de haber realizado la corrección de errores aritméticos y de ordenar las ofertas presentadas de menor a mayor, el Comité de Evaluación procederá a solicitar a los oferentes una explicación detallada de la composición del precio ofertado de cada ítem, rubro o partida adjudicable, cuando los montos cotizados se aparten de los parámetros o rangos establecidos en la normativa aplicable.

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:

Precio del Bien	Gastos de traslado	Gastos administrativos/financieros	Retenciones IVA	Rentabilidad	Precio final

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 normativa aplicable.

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

Certificado de Producto y Empleo Nacional - CPS

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

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

b) Oferentes en Consorcio:

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

b.2. Provisión de Servicios. Todos los integrantes del consorcio deben contar con el CPEN. (Se entenderá por el término “servicio” aquello que comprende a los servicios en general, las consultorías, obras públicas y servicios relacionados a obras públicas).

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

Para los casos de prestación de servicios, el CPEN será intransferible. Se permite el uso del CPEN por terceros exclusivamente en caso de productos y bajo autorización expresa del titular del certificado, éste podrá ser utilizado por terceros para la presentación de ofertas en el marco de un procedimiento de contratación, de acuerdo con lo establecido en la reglamentación respectiva.

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

Margen de preferencia en procedimientos de contratación de carácter internacional

No Aplica

Requisitos documentales para la 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. Declaración jurada de conocimiento de la existencia de un conflicto de intereses respecto a los funcionarios públicos intervinientes en el procedimiento. (**)
5. Certificado de Producto y Empleo Nacional emitido por el MIC, en formato físico, solo en caso de imposibilidad de certificación electrónica. **(**)**

6. Certificado de Cumplimiento Tributario. **(**)**
7. Patente profesional, comercial y/o industrial del municipio en donde esté asentado el establecimiento del oferente. **(**)**
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.
a. Fotocopia simple de los documentos que acrediten la existencia legal de la persona jurídica tales como la Escritura Pública de Constitución, según el tipo de sociedad y protocolización de los Estatutos Sociales. Los estatutos deberán estar inscriptos en la Sección Personas Jurídicas de la Dirección de Registros Públicos. **(*)**
b. Constancia de inscripción en el Registro Único de Contribuyentes. (**)
c. Fotocopia simple de los documentos de identidad de los representantes o apoderados de la sociedad. (*)
d. Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al oferente. Estos documentos pueden consistir en: un poder suficiente en el que conste que el apoderado posee facultades suficientes para representar y obligar a la persona jurídica, otorgado por Escritura Pública (no es necesario que esté inscripto en el Registro de Poderes); o los documentos societarios que justifiquen la representación del firmante, tales como las actas de asamblea y de directorio en el caso de las sociedades anónimas. **(*)**
8.3. Oferentes en Consorcio en formación.

a. Original o fotocopia del acuerdo de intención de constituir el consorcio, en caso de resultar adjudicados y antes de la firma del contrato. (*)
b. Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al consorcio en formación y que acrediten las facultades de los firmantes del acuerdo de intención para consorciarse. Estos documentos pueden consistir en (*): I. Original o fotocopia del acuerdo de intención de constituir el consorcio en caso de resultar adjudicados y antes de la firma del contrato, instrumentado por escritura pública, o II. Original o fotocopia del acuerdo de intención de constituir el consorcio en caso de resultar adjudicados y antes de la firma del contrato, instrumentado por acuerdo privado. Cada integrante del consorcio que sea persona física domiciliada en la República del Paraguay deberá presentar los documentos requeridos para Oferentes Individuales especificados en el apartado Oferentes. (Personas Físicas) y, las personas jurídicas domiciliadas en Paraguay deberán presentar los documentos requeridos para Oferentes (Personas Jurídicas).
c. Un poder en el que conste que el apoderado posee facultades suficientes para representar y obligar al Consorcio, otorgado por escritura pública (no es necesario que esté inscripto en el Registro de Poderes) (*).
8.4. Oferentes en Consorcios constituidos o formalizados.
a. Original o fotocopia del instrumento público (escritura pública) de constitución del consorcio. (*)
b. Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al consorcio. Estos documentos pueden consistir en (*): I.Original o fotocopia del instrumento público (escritura pública) de constitución del consorcio. II. Un poder en el que conste que el apoderado posee facultades suficientes para representar y obligar al Consorcio, otorgado por escritura pública (no es necesario que esté inscripto en el Registro de Poderes).

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

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, y deberán estar vigente a la fecha y hora tope de presentación de oferta.

Los documentos indicados con doble asterisco (**) son considerados documentos formales y deben estar vigentes a la fecha y hora tope de presentación de ofertas. La falta de firma en documentos formales no será un motivo de descalificación, salvo que expresamente se disponga la exigencia de la firma del oferente en cuyo caso la omisión o disconformidad deberá analizarse

conforme a los Artículos 77, 78 y 80 del Decreto 2264/24.

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

Capacidad Financiera

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

1) **Para contribuyentes de IRE GENERAL:** Deberán cumplir con el siguiente parámetro:

- **Ratio de Liquidez**: activo corriente / pasivo corriente. Deberá ser igual o mayor que 1, en promedio, en los años (2023-2024-2025).
- **Endeudamiento**: pasivo total / activo total. No deberá ser mayor a 0,80 en promedio, en los años (2023-2024-2025).
- **Rentabilidad**: Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital. El promedio en los años (2023-2024-2025), no deberá ser negativo.

2) **Para contribuyentes de IRE SIMPLE.** Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso). Deberá ser igual o mayor que 1, el promedio de los años (2023-2024-2025).

4) **Para contribuyentes de exclusivamente IVA General.** Deberá cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso)**.** Deberá ser igual o mayor que 1, el promedio de los años (2023-2024-2025).

Observación: **Para los consorcios**, todos los integrantes del consorcio deberán cumplir con los criterios de capacidad financiera.

Requisitos documentales para la evaluación de la capacidad financiera

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

a	a. Balance General de los ejercicios fiscales cerrados correspondientes a los años 2023, *2024 y 2025,* con su correspondiente Estado de Resultados] - para los contribuyentes del IRE GENERAL
	b. Presentación del Formulario N° 501 años 2023-2024-2025 para los contribuyentes del IRE SIMPLE
	c. Para contribuyentes Formularios IVA General: de los años 2023-2024-2025
	d. Certificado de Cumplimiento Tributario vigente a la fecha y hora tope de presentación de ofertas

Experiencia requerida

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

a. Demostrar la experiencia en **Provisión de Equipos de seguridad de redes** con facturaciones de venta con sus respectivas recepciones finales por un monto equivalente al **40** % como mínimo del monto total ofertado en la presente licitación, de los: **3 últimos** años. *2023, 2024 y 2025*
b. Demostrar la experiencia en **Provisión de Equipos de Networking** con facturaciones de venta con sus respectivas recepciones finales por un monto equivalente al **40** % como mínimo del monto total ofertado en la presente licitación, de los: **3 últimos** años. *2023, 2024 y 2025*
c. Demostrar la experiencia en **Provisión de Licencias** con facturaciones de venta con sus respectivas recepciones finales por un monto equivalente al **40** % como mínimo del monto total ofertado en la presente licitación, de los: **3 últimos** años. *2023, 2024 y 2025*
d. Demostrar la experiencia en **Servicios de soporte Técnico, mantenimiento de hardware** con facturaciones de venta con sus respectivas recepciones finales por un monto equivalente al **40** % como mínimo del monto total ofertado en la presente licitación, de los: **3 últimos** años. *2023, 2024 y 2025*

Para acreditar la experiencia requerida para los items 7 y 8 de las especificaciones tecnicas, el oferente debera cumplir con lo siguiente:

a. Pertenecer a rubros relacionados a Tecnologías de la Información y Comunicación, específicamente a software. Esto deberá verificarse en el objeto de su Constitución, siendo una de las actividades principales o Constancia de RUC.
b. Contar con Mínimo de 2 años de experiencia o antigüedad en el rubro de software demostrable con la presentacion de facturaciones o Actas de recepcion.
c. contar con un Mínimo de 5 referencias de clientes que acrediten los servicios de provision de software, u otros servicios de TIC, acreditables con la presentacion de facturaciones, contratos o constancias firmadas de organizaciones privadas o públicas. Al menos 2 referencias deben corresponder a trabajos realizados en el Paraguay para organizaciones públicas o privadas radicadas en nuestro país.
d. Restricción de monto: deberá cumplir al menos una de las siguientes 2 restricciones:
    - Al menos una referencia de trabajo similar por el 20% del monto referencial de la adquisición, provisto a un mismo cliente.
    - La sumatoria de los montos de las referencias presentadas que cumplan estos criterios deberá ser como mínimo el 40% del monto referencial de la adquisición.
    - Deberá acreditar la autorización del fabricante y condiciones de realizar la instalación, configuración y soporte del software, según lo solicitado en la planilla de especificaciones Técnicas

Observación: Para los consorcios, deberá indicarse en la oferta cuál es la empresa líder del consorcio, quien deberá cumplir con al menos 60% de los criterios de calificación de experiencia, y el 40% restante lo cumplirán el o los demás integrantes del consorcio. En caso que un integrante cumpla el 100 %, se dará por cumplido el requisito

En caso de participación mediante consorcio, al menos uno de sus integrantes deberá cumplir con el cien por ciento (100%) de los requisitos de experiencia requerida y capacidad técnica establecidos para los ítems 7 y 8.

La actividad comercial, industrial o de servicios debe estar vinculada con el tipo de bienes o servicios a contratar

---

Requisitos documentales para la evaluación de la experiencia

1. Copia de facturaciones, contratos y/o recepciones finales que avalen la experiencia requerida.

1. Copia de facturaciones de ventas con sus respectivas recepciones finales que avalen la experiencia requerida para cada items.
2. Carta de referencia de instituciones sobre cumplimiento satisfactorio del contrato sobre la provisión de equipos de seguridad de redes en tiempo y forma.
3. Copia de Constitución o Constancia de RUC 4. Copia de facturas, contratos, recepciones finales, constancias u otros documentos equivalentes que avalen la experiencia requerida.

Se deberá acreditar que el giro comercial de la empresa corresponde al procedimiento de contratación ofertado, para lo cual deberá presentar copia simple y legible del documento que acredite la actividad comercial, industrial o de servicio, pudiendo ser: la constancia de RUC, patente municipal o documentos constitutivos, siempre que de la documentación se desprenda su actividad comercial y la correspondencia al procedimiento objetado. Cuando no resulte aplicable la constancia de RUC, la patente municipal o los documentos constitutivos, el oferente deberá manifestar y justificar esta condición en su oferta y presentar otra documentación a los efectos de acreditar el giro comercial

---

Capacidad Técnica

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

I. El oferente deberá contar con los siguientes profesionales certificados, y los mismos deberán formar parte del plantel del oferente con una antigüedad de al menos 2 (dos) años. No se aceptaran profesionales subcontratados. Serán aceptados profesionales que formen parte de la estructura interna de la empresa en calidad de socios, directores o gerentes de primera línea, debiendo acreditar dicha condición mediante el Acta de Asamblea de Elección de Autoridades o el Estatuto Social debidamente inscripto.

a. Al menos 1 (un) profesional con certificación vigente PMP (Project Management Professional) del PMI (Project Management Institute) o superior.
b. Al menos 1 (un) Técnico certificado por el fabricante de las marcas ofertadas para los ítems del 1 al 6.
c. Al menos 1 (un) Técnico con certificación de nivel medio superior (Ej: CCNP, FCP o similar) en soluciones de Networking
d. Contar con 2 (dos) técnicos con certificación de nivel medio (Ej.: CCNA, FCA o similar) en soluciones de Networking.
e. Contar con al menos 4 (cuatro) técnicos certificados en CompTIA Tech+ o superior.
f. Contar con al menos 1 (un) técnico certificado en CompTIA Security+ o superior.
g. Contar con al menos 1 (un) técnico certificado en CompTIA A+ o superior.
h. Contar con al menos 2 (dos) técnicos en Firewall certificados por la marca ofertada, los cuales deberán contar con experiencia en la implementación, configuración y optimización de firewalls.

II. El oferente deberá presentar una carta de Autorización del Fabricante de los equipos ofertados para los ítems 1.1 al 1.6 (dirigida a la Institución y con referencia al presente proceso de licitación. No se aceptaran cartas genéricas)
III. El oferente deberá presentar una certificación vigente de un sistema de gestión que garantice la seguridad de la información en la prestación de servicios, emitida por una entidad certificadora competente, acreditada y verificable. La certificación deberá contar mínimamente con una (1) recertificación desde su fecha de certificación inicial, manteniéndose vigente a la fecha de presentación de ofertas y deberá evidenciar criterios orientados a asegurar la confidencialidad, integridad y protección de los datos, abarcando mínimamente la integración del hardware, software y servicio de soporte técnico, especializado para el sector público. Dicha certificación deberá

asegurar, como mínimo la implementación de controles y procesos alineados a buenas practicas reconocidas para la gestión de la seguridad, confidencialidad e integridad de la información y de los datos tratados.

IV. Se exigirá la presentación de Certificados ISO 9001:2015 del fabricante para los ítems 1.2 y 1.3
V. Catálogos y especificaciones técnicas del equipo ofertado para los ítems 1.2 y 1.3.
VI. PARA ACREDITAR LOS ITEMS 7 Y 8 el oferente deberá contar con al menos 2 técnicos radicados en el país con experiencia en el uso del software para la instalación/configuración y capacitación, que formará parte del plantel técnico de instalación/soporte

Observación: Para los consorcios, deberá indicarse en la oferta cuál es la empresa líder del consorcio, quien deberá cumplir con al menos 60% de los criterios de calificación de experiencia, y el 40% restante lo cumplirán el o los demás integrantes del consorcio. En caso que un integrante cumpla el 100 %, se dará por cumplido el requisito

En caso de participación mediante consorcio, al menos uno de sus integrantes deberá cumplir con el cien por ciento (100%) de los requisitos de experiencia requerida y capacidad técnica establecidos para los ítems 7 y 8.

Requisitos documentales para evaluar el criterio de capacidad técnica

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

a. Curriculum vitae de los personales propuestos

b. Certificado, o título que acredite que los personales cuentan con las certificaciones requeridas en el numeral I) de la capacidad técnica.

c. Planilla de IPS para acreditar que los personales propuestos forman parte del plantel de la empresa oferente y/o copia de Acta de Asamblea de Elección de Autoridades o el Estatuto Social debidamente inscripto en caso de socios, directores o gerentes de primera linea.

d. Carta de Autorización del Fabricante de los equipos.

e. Certificación vigente de un sistema de gestión emitida por una entidad certificadora competente.

f. Certificado ISO 9001:2015 del fabricante

g. Catálogos y especificaciones técnicas

H. Presentar copias simples de los currículum vitae, certificados, constancias de capacitación o documentaciones equivalentes de los profesionales propuestos PARA ACREDITAR EL ITEM VI

Otros criterios que la convocante requiera

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

Además de la evaluación de los documentos requeridos en los criterios de experiencia y capacidad técnica, el comité evaluador realizara la verificación del cumplimiento de todos los requerimientos exigidos en la planilla de Especificaciones técnicas

Evaluación basada en multiplicidad de criterios

Se deben establecer los criterios de evaluación que serán aplicados al principio de valor por dinero, indicando por cada criterio la siguiente información:

No Aplica

En caso de optar por el método de multiplicidad de criterios deberá estar sujeto a los lineamientos emitidos por el MEF y la DNCP.

Ponderación de criterios de evaluación - Multiplicidad de criterios

La ponderación de cada criterio de evaluación especificado en la cláusula anterior será el siguiente:

No Aplica

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 aritmético.

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

Disconformidades, 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 moneda extranjera con décimos y céntimos la convocante procederá a realizar el redondeo hacia abajo.
d. 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.

Notificación del resultado

La notificación del resultado se realizará a través del SICP de manera automática, desde la comunicación de los documentos en el SICP, a los correos declarados en el Registro de Proveedores del Estado de los oferentes presentados. A efectos de la notificación oficial, solo serán considerados tales correos electrónicos. Dicha notificación, al tiempo de la comunicación de los documentos en el SICP, comprenderá la Resolución del resultado y el informe de evaluación respectivo. La fecha de esta notificación se considera válida a todos los efectos, siempre que se cumplan con las formalidades previstas en el Art. 52 y 55 de la Ley N.º 7021/22 y, lo previsto en el Título V, Capítulo VI, Sección IV y V del Decreto Reglamentario N.º 2264/24.

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

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

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

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

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

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

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 respecto al análisis de su oferta.

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 regirá de conformidad a la cláusula de adendas y convenios modificatorios.

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

Identificación de la unidad solicitante y justificaciones

En este apartado la convocante deberá indicar los siguientes datos:

- *Ing. Nelson Duarte Paris, Gerente de la Unidad de Tecnología de la Información y Comunicación.*
- ***Justificación de la necesidad**: la ANNP con esta adquisición cubrirá la necesidad de poseer una herramienta que podrá facilitar y mejorar las condiciones de manejo de información y general información al momento de realizar trabajos en las distintas Terminales Portuarias y así reducir costos generados en papel y operativos, teniendo una mejor utilización de tiempo ya que las notas podrán ser contestadas con mayor agilidad y celeridad.*
- ***Justificar la planificación**. El llamado responde a planificación única.*
- ***Justificar las especificaciones técnicas establecidas**: las especificaciones técnicas fueron elaborados por técnicos capacitados de la Institución y los requerimientos técnicos han sido definidos con criterios de razonabilidad, objetividad e imparcialidad ajustándose a los estándares internacionales y a la realidad operativa de la Institución.*

Las especificaciones técnicas deberán estar sustentadas en el dictamen técnico, requerido al momento de la comunicación de la convocatoria.

Especificaciones Técnicas "CPS"

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

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

- Las EETT sirven de referencia para verificar el cumplimiento técnico de las ofertas y posteriormente evaluarlas. Por lo tanto, unas EETT bien definidas facilitarán a los oferentes la preparación de ofertas que se ajusten a los documentos de licitación, y a la convocante el examen, evaluación y comparación de las ofertas.

- En las EETT se deberá estipular que todos los bienes o materiales que se incorporen en los bienes deberán ser nuevos, sin uso y del modelo más reciente o actual, y que contendrán todos los perfeccionamientos recientes en materia de diseño y materiales, a menos que en el contrato se disponga otra cosa.

- En las EETT se utilizarán las mejores prácticas. Ejemplos de especificaciones de adquisiciones similares satisfactorias en el mismo sector podrán proporcionar bases concretas para redactar las EETT.

- Las EETT deberán ser lo suficientemente amplias para evitar restricciones relativas a manufactura, materiales, y equipo generalmente utilizados en la fabricación de bienes similares.

- Las normas de calidad del equipo, materiales y manufactura especificadas en los Documentos de Licitación no deberán ser restrictivas. 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”, remitiendo la aclaración respectiva.

- Cuando en las ET se haga referencia a otras normas o códigos de práctica particulares, éstos solo serán aceptables si a continuación de los mismos se agrega un enunciado indicando otras normas emitidas por autoridades reconocidas que aseguren que la calidad sea por lo menos sustancialmente igual.

- Asimismo, respecto de los tipos conocidos de materiales, artefactos o equipos, cuando únicamente puedan ser caracterizados total o parcialmente mediante nomenclatura, simbología, signos distintivos no universales o marcas, únicamente se hará a manera de referencia, procurando que la alusión se adecue a estándares internacionales comúnmente aceptados.

- Las EETT deberán describir detalladamente los siguientes requisitos con respecto a por lo menos lo siguiente:

(a) Normas de calidad de los materiales y manufactura para la producción y fabricación de los bienes.

(b) Lista detallada de las pruebas requeridas (tipo y número).

(c) Otro trabajo adicional y/o servicios requeridos para lograr la entrega o el cumplimiento total.

(d) Actividades detalladas que deberá cumplir el proveedor, y consiguiente participación de la convocante.

(e) Lista detallada de avales de funcionamiento cubiertas por la garantía, y las especificaciones de las multas aplicables en caso de que dichos avales no se cumplan.

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

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

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

Detalle de los bienes y/o servicios

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

Listado del Detalle:

Ítems	LISTA DE BIENES Y SERVICIOS	Unidad de Medida	Cantidad
	ADQUISICIÓN E INSTALACIÓN DE EQUIPOS SE SEGURIDAD FIREWALL, LLAVE EN MANO- que incluye:	**Unidad**	**1**
1	PLATAFORMA GESTIONADO DE DETECCION Y RESPUESTA	Unidad	1
2	EQUIPO DE SEGURIDAD TIPO 1	Unidad	2
3	EQUIPO DE SEGURIDAD TIPO 2	Unidad	13
4	SWITCH CORE	Unidad	2
5	LICENCIAS ANTISPAM	Unidad	200
6	LICENCIAS ENCRIPTACION DE DISPOSITIVOS	Unidad	150
7	LICENCIAS WINDOWS SERVER	Unidad	8
8	LICENCIAS WINDOWS CAL	Unidad	300
9	SERVICIO DE IMPLEMENTACION Y SOPORTE	Unidad	1

GENERALIDADES Y OBJETIVOS

Estas especificaciones tienen por objeto establecer las exigencias que deben tener los equipos, dispositivos y el software necesario para la Modernización del Sistema de Seguridad de la Administración Nacional de Navegación y Puertos (ANNP) orientados a un conjunto de tecnologías, políticas y procedimientos diseñados para proteger la infraestructura de comunicación contra accesos no autorizados, pérdida de datos y ciberataques.

Situación actual

La infraestructura actual de red y seguridad perimetral presenta deficiencias que comprometen la

disponibilidad, el rendimiento y la protección de la red con los siguientes problemas principales:

- **Ausencia de alta disponibilidad real** en el sistema de seguridad perimetral, generando un punto único de falla ante incidentes, mantenimiento o fallas de hardware.
- Capacidad limitada de los equipos de seguridad actuales para **analizar tráfico cifrado, aplicaciones críticas y amenazas avanzadas**, lo que incrementa el riesgo de intrusiones, malware y accesos no autorizados.
- Infraestructura de core de red sin esquemas de **redundancia y tolerancia a fallos**, afectando la continuidad de los servicios ante fallas en los equipos de conmutación.
- Falta de **integración entre seguridad perimetral y el núcleo de red**, dificultando una gestión homogénea, segura y de alto desempeño del tráfico corporativo.
- Crecimiento sostenido de usuarios, servicios y aplicaciones que **supera la capacidad actual** de la infraestructura, impactando en la performance y la estabilidad operativa.
- **Falta de gerenciamiento centralizado de la red y de los eventos de seguridad**, dificultando la visibilidad en tiempo real del estado de la infraestructura, el tráfico y las amenazas.
- Ausencia de un **servicio de monitoreo continúo especializado**, que permita la detección temprana, análisis y respuesta ante incidentes de seguridad de manera proactiva.
- Dependencia de atención reactiva ante incidentes, sin un esquema formal de **asistencia técnica avanzada y respuesta coordinada**.
- Incremento del tráfico de red, usuarios remotos y aplicaciones críticas que supera las capacidades actuales de control, monitoreo y protección.

Estas condiciones elevan significativamente el riesgo de incidentes de ciberseguridad, reducen la capacidad de respuesta ante amenazas avanzadas y comprometen la disponibilidad de los servicios críticos de la organización.

Con el objetivo de fortalecer la seguridad, disponibilidad y gestión de la red corporativa, la **Administración Nacional de Navegación y Puertos** se propone la **modernización y la implementación de una plataforma integral de seguridad de red**, que combine infraestructura redundante, protección avanzada y servicios de monitoreo y respuesta especializada.

La solución propuesta por el oferente deberá estar diseñada para eliminar puntos únicos de falla, mejorar la capacidad de gestión y garantizar una respuesta eficaz ante incidentes de ciberseguridad, tanto en la sede central como en las filiales ubicadas en el interior del país.

1. Seguridad perimetral en alta disponibilidad

La solución debe basarse en la implementación de una **solución de seguridad perimetral redundante**, compuesta por **dos (2) dispositivos de seguridad de próxima generación**, configurados en un **esquema de Alta Disponibilidad (HA)**.

Esta arquitectura debe permitir:

- Conmutación automática ante fallas de hardware o software.
- Continuidad operativa de los servicios de red sin interrupciones.
- Inspección avanzada del tráfico, control de aplicaciones y protección frente a amenazas externas.
- Integración directa con el núcleo de red corporativo.

2. Seguridad para filiales en el interior del país

Con el fin de unificar las políticas de seguridad y extender la protección de la **Administración Nacional de Navegación y Puertos**, se deberá contemplar la provisión de **trece (13) dispositivos de seguridad perimetral** destinados a las filiales ubicadas en el interior del país.

Estos equipos permitirán:

- Establecer perímetros de seguridad locales.
- Aplicar políticas homogéneas de control y protección.
- Asegurar la conectividad segura entre sedes mediante túneles cifrados.
- Centralizar la gestión y el monitoreo de la seguridad de todas las ubicaciones.

3. Core de red corporativa redundante

La solución deberá incluir la modernización del núcleo de la red mediante la implementación de un **core de red redundante**, compuesto por **dos (2) switches de núcleo** configurados en alta disponibilidad.

Este diseño permitirá:

- Eliminar puntos únicos de falla en la capa de conmutación.

- Soportar enlaces de alta capacidad y agregación de enlaces.
- Garantizar estabilidad, alto rendimiento y escalabilidad.
- Integrar de forma segura la infraestructura de red con la plataforma de seguridad perimetral.

4. Servicio de detección y respuesta gestionada

Como parte fundamental de la solución, se deberá proponer la provisión de un **servicio de detección y respuesta gestionada**, orientado a suplir las actuales deficiencias de gerenciamiento y asistencia técnica especializada.

El servicio deberá contemplar:

- **Monitoreo continuo 24x7** de eventos de seguridad y actividad de red.
- Detección temprana de amenazas avanzadas y comportamientos anómalos.
- Análisis, contención y mitigación de incidentes de seguridad.
- Asistencia técnica especializada por equipos dedicados.
- Reportes periódicos, alertas y recomendaciones de mejora continua.
- Reducción significativa de los tiempos de detección y respuesta ante incidentes.

5. Servicios adicionales de protección

La propuesta deberá incorporar todas las licencias adicionales que fortalezcan la postura de seguridad de la organización como:

- **Protección contra correo malicioso y spam**, reduciendo riesgos asociados a phishing, malware y fraudes por correo electrónico.
- **Cifrado de dispositivos**, garantizando la protección de la información almacenada en equipos corporativos ante pérdida, robo o accesos no autorizados.

6. Modalidad de provisión Llave en mano

El **Oferente** deberá proveer la solución bajo la modalidad **llave en mano**, siendo responsable de la ejecución integral del proyecto, incluyendo, como mínimo:

- Provisión de todos los **equipos, licencias y componentes necesarios**.
- **Mano de obra completa para la implementación**, instalación, configuración y puesta en producción del sistema de seguridad y del core de red.
- Integración de todos los componentes (firewalls, core de red, filiales y servicios de seguridad).
- **Acompañamiento técnico especializado** durante todas las etapas del proyecto.
- Soporte durante el período de estabilización posterior a la puesta en marcha.
- **Capacitación y entrenamiento al personal de GTIC de la Administración Nacional de Navegación y Puertos**, orientada a la operación, administración básica y buenas prácticas de seguridad del sistema implementado.
- Entrega de documentación técnica básica de la solución implementada.

6. Beneficios de la solución

- Alta disponibilidad y resiliencia de la infraestructura de red y seguridad.
- Gestión centralizada y visibilidad completa del entorno.
- Protección integral de la sede central y las filiales.
- Asistencia técnica especializada y respuesta proactiva ante amenazas.
- Mejora de la continuidad operativa y reducción del riesgo institucional.
- Infraestructura escalable y preparada para el crecimiento futuro.

ESPECIFICACIONES TECNICAS

1 - PLATAFORMA GESTIONADO DE DETECCION Y RESPUESTA			
Descripción	**Descripción Técnica**	**Mínimo exigido**	**Ofertado**

Marca	Especificar		
Modelo	Especificar		
Procedencia	Especificar		
Cantidad	1(uno) unidad		
Alcance	La plataforma deberá incluir: -Al menos 500 licencias para enpoints. -Al menos 5 licencias para servidores.	Exigido	
1. Requerimientos Generales	1.1 Se requiere el suministro de un servicio gestionado de detección y respuesta de seguridad (MDR) que opere 24x7.	Exigido	
	1.3 La plataforma debe permitir a los analistas de seguridad de la Entidad visualizar dashboards, investigaciones y demás gestiones realizadas por el equipo MDR, todo dentro de una misma interfaz unificada y una única plataforma, sin necesidad de cambiar de entorno ni consola.	Exigido	
	1.4 EL servicio MDR debe escalar investigaciones completas, no alertas ni detecciones aisladas.	Exigido	
	1.5 El servicio de MDR debe incluir análisis de amenazas detectadas, investigaciones proactivas y acciones de respuesta definidas y documentadas.	Exigido	
	1.6 El servicio de MDR debe ejecutar acciones de respuesta proactiva basadas en playbooks predefinidos desde la plataforma.	Exigido	
	1.7 El servicio de MDR debe incluir capacidades de threat hunting proactivo mensual, basado en inteligencia de amenazas actuales y tácticas observadas en casos reales de respuesta a incidentes.	Exigido	
	1.8 El servicio de MDR debe suministrar un canal de comunicación directa con analistas expertos desde la plataforma XDR para asistencia inmediata y colaboración con un tiempo de respuesta menor o igual a 90 segundos.	Exigido	

	1.9 El proveedor debe asignar un Customer Success Manager que realice revisiones trimestrales del servicio y recomiende mejoras a la postura de seguridad de la Entidad.	Exigido	
	1.10 El servicio MDR debe incluir monitoreo continuo 24x7 del entorno de la Entidad, utilizando flujos de trabajo guiados y analítica avanzada basada en ciencia de datos.	Exigido	
2. Requerimientos de Respuesta a Incidentes	2.1 La suscripción MDR deberá contemplar respuesta ilimitada para los activos en alcance, entendida como actividades de contención y mitigación gestionadas desde la consola de la Plataforma.	Exigido	
	2.2 El equipo de respuesta a incidentes debe proporcionar respuesta ilimitada ante incidentes de seguridad sobre los activos definidos de la Entidad, incluyendo, como mínimo:	Exigido	
	- Análisis de endpoints, utilizando la telemetría recibida activamente en la plataforma.	Exigido	
	- Análisis de red, a partir de sensores integrados con la plataforma.	Exigido	
	- Análisis de código malicioso, sobre muestras de malware identificadas durante la investigación.	Exigido	
	- Análisis de registros (logs), limitados a aquellos provenientes de integraciones compatibles y activas en la plataforma.	Exigido	
	- Evaluación de datos de triage de los endpoints que estén enviando telemetría en tiempo real.	Exigido	
	- Ejecución de acciones de respuesta.	Exigido	
3. Panel de Control Servicio MDR	3.1 El proveedor MDR debe ofrecer un panel de control con widgets que permitan visualizar la actividad, valor generado y métricas del servicio gestionado. Este panel debe ser accesible por los administradores de la Entidad y debe incluir como mínimo:	Exigido	
	3.1.1 Canal de Eventos	Exigido	

	- Visualización del número de alertas generadas por eventos crudos.	Exigido	
	- Visualización de nuevas investigaciones iniciadas a partir de las alertas.	Exigido	
	- Número de investigaciones entregadas al cliente para acción	Exigido	
	2.1.2 Investigaciones en curso	Exigido	
	- Visualización de investigaciones activas, abiertas o pendientes de acción.	Exigido	
	- Debe permitir colaborar con analistas y hacer seguimiento del estado.	Exigido	
	3.1.3 Tiempos de Respuesta: El servicio de MDR debe presentar métricas que reflejen la eficiencia del servicio:	Exigido	
	- Tiempo medio de entrega: desde creación hasta envío de investigación.	Exigido	
	- Tiempo medio de reconocimiento: desde el envío hasta la apertura por el cliente.	Exigido	
	- Tiempo medio de resolución: desde el envío hasta cierre por parte del cliente.	Exigido	
	3.1.4 Investigaciones Completadas	Exigido	
	- Total de investigaciones completadas en el período seleccionado.	Exigido	
	- Comparativa porcentual con el período anterior.	Exigido	
	- Gráfico de barras por categoría: Falsos positivos, Verdaderos positivos, No concluyentes y Desconocidos.	Exigido	
	3.1.5 Incidentes de Seguridad Confirmados	Exigido	

	- Visualización de investigaciones con código de cierre de Incidente de seguridad confirmado.	Exigido	
	- Clasificación por vector de acceso inicial (MITRE ATT&CK).	Exigido	
	· Tendencias por categoría y período.	Exigido	
	3.1.6 Falsos Positivos	Exigido	
	- Número total de falsos positivos en el período seleccionado.	Exigido	
	- Comparativa con los tres períodos anteriores.	Exigido	
	- Desglose por detector generador de alerta.	Exigido	
	- Proporción de alertas por tipo de detector en gráfico circular.	Exigido	
Carta de Autorización	Carta de Distribución del Representante / Distribuidor Local y del Fabricante de la plataforma ofertado. Demostrar la cadena de autorizaciones desde el Fabricante hasta el Oferente de los Equipos con referencia al proceso.	Exigido	
Instalación, configuración y soporte	El oferente deberá de incluir en su oferta todos los materiales, mano de obra, configuraciones para la puesta en marcha y correcto funcionamiento de la plataforma.	Exigido	
Acuerdo de Confidencialidad	El proveedor adjudicado, así como su personal y cualquier tercero que participe en la prestación del servicio MDR, deberá suscribir un Acuerdo de Confidencialidad (NDA) respecto de toda la información técnica, operativa, documental y de seguridad a la que tenga acceso durante la ejecución del contrato	Exigido	

Residencia y Jurisdicción de los Datos	El oferente deberá declarar en su propuesta la ubicación geográfica de los centros de datos donde serán almacenados, procesados o respaldados los datos generados por la plataforma MDR y su consola de gestión. el proveedor deberá informar las políticas de retención, respaldo, eliminación y recuperación de datos aplicables a la plataforma MDR.		
Notificación de Incidentes del Proveedor	El proveedor deberá notificar a la convocante cualquier incidente de seguridad que afecte a la infraestructura utilizada para la prestación del servicio MDR, incluyendo la plataforma cloud, consolas de administración, sistemas de almacenamiento, repositorios de telemetría o mecanismos de autenticación asociados al servicio. La notificación deberá realizarse en un plazo no mayor a veinticuatro (24) horas desde la detección del incidente y deberá contener, como mínimo, una descripción preliminar del evento, los activos afectados, el impacto conocido o potencial sobre la información o servicios de la convocante y las medidas iniciales de contención adoptadas.		

2 - EQUIPO DE SEGURIDAD TIPO 1			
Descripción	**Descripción Técnica**	**Mínimo Exigido**	**Ofertado**
Cantidad:	2 (dos) unidades		
Marca:	Especificar		
Modelo:	Especificar		
Procedencia:	Especificar		
Hardware	Procesador: Dos procesadores para diferentes fines, un procesador deber ser de tipo Flow Processor (NPU)	Exigido	
	RAM: 8 GB DDR4	Exigido	

Almacenamiento: 2 x SSD de al menos 200 GB (en RAID)	Exigido	
Puertos Ethernet:	Exigido	
4xGbE cobre +		
4x2.5GbE cobre +		
6x10GbE SFP+		
se deberán proveer con cada equipo 6 (seis) transceivers SFP+ 10GBASE-SR LC Duplex multimodo.		
Puertos de E/S:	Exigido	
2x COM (RJ45 y Micro USB)		
2x USB 3.0		
Fuente de alimentación: Auto-Ranging interno 110-240VAC, 50-60Hz. Hot Swap con alimentación redundante incluido	Exigido	
Certificaciones de productos (Safety, EMC): CB, CE, FCC Clase A, VCCI, RCM, UL, CCC	Exigido	
Firewall Throughput - 78.000 Mbps	Exigido	
IPS throughput 35.500 Mbps	Exigido	
VPN throughput - 73.000 Mbps	Exigido	
Throughput contra amenazas 30.000 Mbps	Exigido	
Conexiones simultáneas 16.000.000	Exigido	
Nuevas conexiones/seg - 400.000	Exigido	
Máximo de usuarios con licencia: sin restricciones	Exigido	

Características del firewall base	Interfaz de usuario optimizada y diseñada específicamente para grandes conjuntos de reglas de un vistazo e indicadores de cumplimiento.	Exigido	
	Soporte de autenticación en dos factores (contraseña única) para acceso de administrador, portal de usuario, IPSec y SSL VPN.	Exigido	
	Herramientas avanzadas de resolución de problemas en GUI (por ejemplo, captura de paquetes).	Exigido	
	Soporte de alta disponibilidad (HA) para agrupar dos dispositivos en modo activo-activo o activo-pasivo con configuración de HA rápida plug-and-play según sea requerido.	Exigido	
	Interfaz de línea de comandos completa (CLI) accesible desde la GUI.	Exigido	
	Administración basada en roles.	Exigido	
	Notificación de actualización de firmware automatizada con un sencillo proceso de actualización automática y funciones de reversión.	Exigido	
	Definiciones de objetos del sistema reutilizables para redes, servicios, hosts, períodos de tiempo, usuarios y grupos, clientes y servidores.	Exigido	
	Portal de usuarios de autoservicio.	Exigido	
	Seguimiento de cambios en configuración.	Exigido	
	Control de acceso de dispositivos flexible para servicios por zonas.	Exigido	
	Opciones de notificación por correo electrónico o SNMP.	Exigido	
	Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.	Exigido	
	Compatibilidad con SNMPv3 y Netflow.	Exigido	

	Soporte de administración central a través de la consola unificada basada en la nube.	Exigido	
	Notificaciones automáticas por correo electrónico para cualquier evento importante.	Exigido	
	Configuraciones de copia de seguridad y restauración: localmente o correo electrónico; bajo demanda, diario, semanal o mensual.	Exigido	
	API para integración de terceros.	Exigido	
	Opción de acceso remoto para el soporte del Fabricante.	Exigido	
	Gestión de licencias basada en la nube a través de un portal de licencias del Fabricante.	Exigido	
	Soporte de Syslog.	Exigido	
	Monitoreo de flujo en tiempo real.	Exigido	
	Indicadores o Alertas de estilo semáforo.	Exigido	
	Interacción rápida y detallada con cualquier widget del centro de control.	Exigido	
	SNMP con una MIB personalizada y soporte para túneles VPN IPSec.	Exigido	
	Soporte para nuevas instancias de AWS (C5 / M5 y T3)	Exigido	
	Soporte de zona WAN virtual en puertas de enlace personalizadas para el uso de un solo brazo posterior a la implementación.	Exigido	
Gestión de Firewall	La solución debe permitir la gestión de los equipos Firewall y los informes de estos equipos (7 días o superior), desde una sola consola de gestión basada en la nube, donde, además, esta consola debe de proporcionar gestión de políticas por grupos de equipos.	Exigido	

	La gestión de políticas de grupo debe permitir que los objetos, la configuración y las políticas se modifiquen una vez y se sincronicen automáticamente con todos los Firewall del grupo.	Exigido	
	La consola debe proporcionar una pista de auditoría histórica completa y un seguimiento del estado de los cambios en las políticas del grupo.	Exigido	
	La consola además debe permitir la gestión de firmware de los equipos, así como el respaldo de los últimos cinco archivos de configuración para cada firewall.	Exigido	
	Las actualizaciones de firmware se deben ofrecen al administrador de la consola de tal manera que con un solo clic se pueda aplicar dicha actualización a cualquier dispositivo manejado dentro de la consola.	Exigido	
	La solución debe permitir implementaciones Zero-Touch desde esta consola central, permitiendo exportar la configuración para cargarla en un dispositivo desde una unidad flash, conectando así automáticamente al dispositivo a la consola central.	Exigido	
	Debe permitir la programación de actualizaciones de firmware	Exigido	
	Debe permitir la generación de Informes de múltiples firewalls.	Exigido	
	Debe además permitir guardar, programar y exportar informes desde esta consola central.	Exigido	
	Esta Consola de gestión debe ser sin ningún costo	Exigido	
	Deberá contar con la capacidad de integrarse con sistemas de monitoreo Open Source.	Exigido	
Firewall, Networking & Routing	El Firewall debe permitir una inspección profunda de paquetes donde todos paquetes deben ser inspeccionados por los motores de IPS, web, AV, control de aplicaciones e inspección SSL, utilizando un motor DPI (Deep Packet Inspection) de transmisión de alto rendimiento y sin proxy.	Exigido	

El Firewall debe contar con Inspección TLS de alto rendimiento, debe contar con compatibilidad de TLS 1.3 sin degradación, políticas de nivel empresarial independientes del puerto, debe permitir una visibilidad única desde el panel de control así resolución de problemas de compatibilidad.	Exigido	
El Firewall debe acelerar el tráfico de SaaS, SD-WAN y tráfico en la nube como: VoIP, video y otras aplicaciones confiables	Exigido	
El Firewall debe contar con una tecnología que le permita descargar el tráfico de forma inteligente para transferir el tráfico confiable a altas velocidades. La descarga de este tráfico se deberá controlar mediante una política para acelerar el tráfico importante de aplicaciones en la nube, o de forma inteligente en función de las características del tráfico.	Exigido	
Debe contar con una lista de excepciones pre empaquetada.	Exigido	
Debe cubrir todos los puertos / protocolos.	Exigido	
Debe admitir todas las suites de cifrado modernas.	Exigido	
La solución debe proporcionar políticas basadas en usuarios, grupos, horarios o redes.	Exigido	
La solución debe proporcionar políticas de tiempo de acceso por usuario / grupo.	Exigido	
La solución deberá hacer cumplir las políticas en zonas, redes o por tipo de servicio.	Exigido	
La solución deberá contar con un firewall basado en zonas.	Exigido	
Deberá proporcionar las zonas predeterminadas para LAN, WAN, DMZ, LOCAL, VPN y WiFi.	Exigido	
La solución deberá permitir el soporte completo de VLAN.	Exigido	
Deberá permitir el aislamiento de zonas y VLAN.	Exigido	

La solución deberá permitir la microsegmentación y autoaislamiento mediante seguridad sincronizada.	Exigido	
Deberá permitir personalizar zonas en LAN o DMZ.	Exigido	
La solución de Firewall deberá permitir la creación de políticas NAT personalizables con enmascaramiento de IP y soporte completo de objetos para redirigir o reenviar múltiples servicios en una sola regla con un asistente de reglas para crear rápida y fácilmente reglas NAT complejas con solo unos pocos clics.	Exigido	
La solución deberá contar con protección flood: bloqueo DoS, DDoS y escaneo de puertos.	Exigido	
Deberá permitir el bloqueo de país por geo-IP.	Exigido	
La solución deberá ofrecer enrutamiento avanzado: estático, multidifusión (PIM-SM) y dinámico (RIP, BGP, OSPF) con compatibilidad total con VLAN 802.1Q	Exigido	
Deberá permitir el enrutamiento de multidifusión independiente del protocolo con snooping IGMP.	Exigido	
La solución deberá contar con soporte y etiquetado de VLAN DHCP.	Exigido	
La solución deberá contar con soporte Jumbo Frame.	Exigido	
La solución de Firewall deberá permitir el equilibrio de enlace SD-WAN: múltiples conexiones a Internet, verificación de estado de enlace automático, conmutación por error automática, equilibrio automático y ponderado y reglas granulares de múltiples rutas.	Exigido	
La solución deberá permitir la configuración completa de DNS, DHCP y NTP.	Exigido	
Deberá permitir DNS dinámico (DDNS).	Exigido	
Deberá contar con la certificación de aprobación del programa de logotipo IPv6 Ready.	Exigido	

	La solución deberá brindar soporte de tunelización IPv6 que incluye implementación rápida 6in4, 6to4, 4in6 e IPv6 (6rd) a través de IPSec.	Exigido	
SD-WAN	La solución deberá permitir el soporte para múltiples opciones de enlace WAN, incluyendo VDSL, DSL, cable y celular 3G / 4G / LTE con monitoreo esencial, balanceo, failover y fail-back".	Exigido	
	Selección de ruta de aplicación y enrutamiento, que se utiliza para garantizar la calidad y minimizar la latencia para aplicaciones de misión crítica como VoIP.	Exigido	
	SD-WAN sincronizada: La solución de firewall debe garantizar la integración con el Antivirus del mismo fabricante permitiendo sincronizar la seguridad de ambos componentes para así aprovechar la claridad y confiabilidad de la identificación de aplicaciones que viene con el intercambio de información entre los puntos finales administrados y el firewall.	Exigido	
	La solución deberá permitir el enrutamiento sincronizado de aplicaciones SD-WAN a través de enlaces preferidos a través de reglas de firewall o enrutamiento basado en políticas.	Exigido	
	Deberá permitir la implementación asequible, flexible y sin intervención o con poca intervención.	Exigido	
	Deberá contar con soporte VPN robusto que incluye IPSec y SSL VPN	Exigido	
	Deberá permitir la orquestación de VPN centralizada	Exigido	
	Integración con Azure Virtual WAN para una red de superposición SD-WAN completa	Exigido	
Cuotas y configuración de Traffic Shaping	La solución deberá permitir configurar "Traffic Shaping (QoS) en la red o basado en el usuario (con opciones mejoradas de tráfico web y de aplicaciones incluidas con la suscripción del mismo fabricante).	Exigido	
	Deberá permitir establecer cuotas de tráfico basadas en el usuario en carga / descarga o tráfico total y cíclico o no cíclico.	Exigido	
	Deberá permitir la optimización de VoIP en tiempo real.	Exigido	

Protección y Control Wireless	La solución deberá permitir una implementación simple plug-and-play de los puntos de acceso inalámbricos (AP), que permita automáticamente aparezcan disponibles en el centro de control del firewall para su administración.	Exigido	
	Deberá permitir el alto rendimiento con el último estándar inalámbrico 802.11ac.	Exigido	
	Deberá contar con un monitoreo y administración centralizadas para los AP y clientes inalámbricos a través del controlador inalámbrico incorporado.	Exigido	
	Puente de AP a LAN, VLAN o una zona separada con opciones de aislamiento de clientes.	Exigido	
	Deberá poseer la compatibilidad con varios SSID por radio, incluidos los SSID ocultos.	Exigido	
	Deberá brindar soporte para los últimos estándares de seguridad y cifrado, incluidos WPA2 Personal y Enterprise.	Exigido	
	Deberá permitir la opción de selección de ancho de canal.	Exigido	
	Deberá permitir el soporte para IEEE 802.1X (autenticación RADIUS) con soporte para servidor primario y secundario.	Exigido	
	Deberá permitir el soporte para 802.11r (transición rápida).	Exigido	
	La solución deberá permitir la creación de cupones (personalizados), contraseña del día o aceptación de T&C.	Exigido	
	Deberá permitir el acceso a Internet de invitados con acceso a la red inalámbrica basada en el tiempo.	Exigido	
	La solución deberá permitir el modo de red en malla y repetición inalámbrica con Aps admitidos.	Exigido	
	Deberá optimizar la selección automática de canales.	Exigido	

	Deberá contar con soporte para inicio de sesión HTTPS.	Exigido	
	La solución deberá tener la capacidad de detección de puntos de acceso no autorizados.	Exigido	
Autenticación	La solución deberá permitir la autenticación a través de: Active Directory, eDirectory, RADIUS, LDAP y TACACS +.	Exigido	
	Deberá brindar agentes de autenticación para Active Directory, SSO	Exigido	
	La solución deberá contar con un inicio de sesión único: Active Directory, eDirectory, RADIUS.	Exigido	
	La consola deberá permitir la autenticación de dos factores (2FA) y autenticación multifactor (MFA)	Exigido	
	Deberá permitir la compatibilidad con los agentes de autenticación de cliente para Windows, Mac OS X, Linux 32/64.	Exigido	
	Deberá contar con la autenticación SSO del navegador: autenticación de proxy transparente (NTLM) y Kerberos.	Exigido	
	Deberá brindar un portal cautivo de inicio de sesión en los navegadores.	Exigido	
	La solución deberá contar con certificados de autenticación para iOS y Android.	Exigido	
	Deberá permitir servicios de autenticación para IPSec, SSL, L2TP.	Exigido	
	Deberá contar con soporte de autenticación de Google Chromebook para entornos con Active Directory.	Exigido	
	Deberá contar con autenticación basada en API.	Exigido	
	Deberá soportar Integración con Azure AD.	Exigido	
	Soporte para crear usuarios con formato UPN para autenticación RADIUS.	Exigido	

Portal de Autoservicio de usuarioWAF	Los usuarios podrán descargar el cliente de autenticación desde la consola en la nube del mismo fabricante.	Exigido	
	Los usuarios a través de la consola central podrán descargar el cliente de acceso remoto SSL (Windows) y los archivos de configuración.	Exigido	
	El portal deberá permitir a los usuarios la opción de cambiar nombre de usuario y contraseña.	Exigido	
	El portal de autoservicio deberá permitir ver el uso personal de Internet.	Exigido	
	El portal deberá permitir acceder a mensajes en cuarentena y administrar listas de remitentes de bloqueo / permiso basadas en usuarios	Exigido	
Opciones de VPN	La solución de Firewall deberá permitir crear túneles VPN IPSec y SSL ilimitados.	Exigido	
	La solución de Firewall deberá permitir crear VPN de sitio a sitio: SSL, IPSec, PFS, RSA, certificados X.509, con clave previamente compartida.	Exigido	
	Deberá brindar soporte a protocolos L2TP.	Exigido	
	Deberá permitir las VPN basada en rutas.	Exigido	
	Deberá permitir el acceso remoto con: SSL, IPsec, iPhone / iPad / Cisco / Soporte de cliente VPN de Android.	Exigido	
	Deberá brindar soporte al protocolo IKEv2 que se utiliza para negociar una asociación de seguridad al principio de una sesión.	Exigido	
	La solución deberá permitir a los usuarios la descarga del cliente SSL para Windows y la descarga de la configuración a través del portal de usuarios del mismo fabricante.	Exigido	
	La solución deberá permitir la aplicación de TLS 1.2 para túneles VPN de acceso remoto y sitio a sitio SSL.	Exigido	

Cliente IPSec	El cliente VPN deberá permitir el soporte de IPSec y SSL.	Exigido	
	El cliente de VPN deberá aprovisionarse e implementarse de una manera sencilla.	Exigido	
	La solución de Firewall deberá permitir el uso de licencias de acceso remoto SSL ilimitadas incluidas sin cargo adicional.	Exigido	
	Deberá contar con la autenticación: Clave pre compartida (PSK), PKI (X.509), Token y XAUTH.	Exigido	
	Deberá contar con un túnel dividido inteligente para un enrutamiento óptimo del tráfico.	Exigido	
	Deberá permitir el soporte NAT-transversal.	Exigido	
	El cliente VPN deberá permitir al cliente descripción gráfica del estado de la conexión.	Exigido	
	El cliente VPN deberá contar con soporte para sistema operativos Mac y Windows.	Exigido	
	Deberá contar con aprovisionamiento de políticas IPSec de acceso remoto con el cliente VPN del mismo fabricante.	Exigido	
	La solución deberá contar con soporte grupal para el cliente VPN que permita importaciones desde AD / LDAP, etc.	Exigido	
Prevención de Intrusiones	La solución deberá proveer un motor de inspección profunda de paquetes IPS de próxima generación y alto rendimiento con patrones IPS selectivos que se permitan aplicar sobre la base de una regla de firewall para obtener el máximo rendimiento y protección.	Exigido	
	La solución deberá proveer la protección contra amenazas de día cero.	Exigido	
	La solución deberá permitir el soporte para firmas IPS personalizadas.	Exigido	

	La solución deberá permitir filtros inteligentes de políticas IPS, esto permite a las políticas dinámicas actualizarse automáticamente a medida que se agregan nuevos patrones.	Exigido	
Protección ATP y Sincronización de los Sistemas de Seguridad	La solución deberá proveer la protección contra amenazas avanzada (detecta y bloquea el tráfico de red que intenta contactar con los servidores de comando y control mediante DNS de varias capas, AFC y firewall).	Exigido	
	La solución deberá garantizar la integración con el Endpoint Protection que permita al Firewall identificar instantáneamente los puntos finales comprometidos, incluidos el host, el usuario, el proceso, el recuento de incidentes y el momento del compromiso.	Exigido	
	Limitar el acceso a los recursos de red o aislar completamente los sistemas comprometidos hasta que se limpien.	Exigido	
	Prevenir los movimientos laterales y que aísle los sistemas comprometidos automáticamente en los puntos finales administrados por el antivirus.	Exigido	
VPN sin cliente	La solución deberá permitir a los usuarios acceder al portal de autoservicio HTML5 cifrado único con soporte para RDP, HTTP, HTTPS, SSH y VNC.	Exigido	
Compatibilidad	Deberá ser de la misma marca del Sistema de gestion a suministrar en este llamado para permitir la máxima compatibilidad de los componentes	Exigido	
Características de protección web	La solución deberá proveer una protección completamente transparente para antimalware y filtrado web.	Exigido	
	La solución deberá contar con la protección avanzada contra amenazas mejorada.	Exigido	
	La solución deberá proveer una base de datos de filtrado de URL con millones de sitios en 92 categorías respaldados por OEMLabs o motores distintos con capacidades equivalentes.	Exigido	
	La solución deberá permitir configurar políticas de tiempo de cuota de navegación por usuario / grupo	Exigido	

La solución deberá permitir configurar políticas de tiempo de acceso por usuario / grupo	Exigido	
La solución deberá permitir configurar el escaneo de malware para bloquear todas las formas de virus, malware web, troyanos y spyware en HTTP / S, Co y correo electrónico basado en la web.	Exigido	
Protección avanzada contra malware web con emulación de JavaScript.	Exigido	
Búsquedas en la nube en tiempo real para obtener la inteligencia de amenazas más reciente.	Exigido	
La solución de Firewall deberá proveer un segundo motor de detección de malware independiente para escaneo dual.	Exigido	
La solución deberá permitir el escaneo en tiempo real o en modo por lotes.	Exigido	
La solución deberá permitir configurar el escaneo HTTP y HTTPS por usuario o por política de red con reglas y excepciones personalizables.	Exigido	
La solución deberá permitir el almacenamiento en caché de contenido web de alto rendimiento.	Exigido	
Filtrado de tipo de archivo por tipo mime, extensión y tipos de contenido activo (por ejemplo, Activex, applets, cookies, etc.)	Exigido	
La solución deberá permitir configurar SafeSearch (basada en DNS) para los principales motores de búsqueda por política (usuario / grupo).	Exigido	
La solución deberá permitir el bloqueo de aplicaciones potencialmente no deseadas (PUA)	Exigido	
La solución deberá permitir configurar el filtrado web automático de sitios identificados por Internet Watch Foundation (IWF) que contienen abuso sexual infantil.	Exigido	

Visibilidad de Aplicaciones en la Nube	El Firewall deberá mostrar la cantidad de datos cargados y descargados en aplicaciones en la nube categorizadas como nuevas, autorizadas, no autorizadas o toleradas.	Exigido	
	La solución deberá permitir obtener detalles sobre usuarios, tráfico y datos de una manera profunda.	Exigido	
	La solución deberá permitir el acceso con un clic a las políticas de configuración del tráfico.	Exigido	
	La solución deberá permitir el filtro para el uso de aplicaciones en la nube por categoría o volumen	Exigido	
	La solución brindará un informe detallado y personalizable de uso de aplicaciones en la nube para informes históricos.	Exigido	
Protección y Control de Aplicaciones	La solución deberá permitir el control de aplicaciones para identificar, clasificar y controlar automáticamente todas las aplicaciones desconocidas de Windows y Mac en la red al compartir información entre los puntos finales y el firewall.	Exigido	
	La solución deberá permitir el control de aplicaciones basado en firmas con patrones para miles de aplicaciones.	Exigido	
	La solución brindará visibilidad y control de aplicaciones en la nube.	Exigido	
	La solución deberá permitir configurar filtros inteligentes de control de aplicaciones que habilitan políticas dinámicas que se actualizan automáticamente a medida que se agregan nuevos patrones.	Exigido	
	La solución deberá permitir configurar control de aplicaciones basado en categoría, características (por ejemplo, ancho de banda y consumo de productividad), tecnología (por ejemplo, P2P) y nivel de riesgo.	Exigido	
	La solución deberá permitir la aplicación de políticas de control de aplicaciones por reglas de usuario o de red.	Exigido	

	La solución debe garantizar la integración con Endpoint con el fin de identificar y sincronizar aplicaciones desconocidas que se estén ejecutando en la red permitiendo la administración y control de la misma. El firewall debe permitir al administrador cambiar el nombre y personalizar esas aplicaciones. Asignar aplicaciones a filtros de aplicaciones para controlar su tráfico.	Exigido	
Web & App Traffic Shaping	La solución deberá permitir configurar opciones personalizadas de Traffic Shaping (QoS) por categoría web o aplicación para limitar o garantizar la carga / descarga o la prioridad total del tráfico y la tasa de bits de forma individual o compartida.	Exigido	
Logging y Reportería	Informes predefinidos con opciones de personalización flexibles.	Exigido	
	Informes para firewalls desde un único punto central (hardware, software, virtual y en la nube) hasta para 30 días.	Exigido	
	La interfaz de usuario deber ser intuitiva y proporcionar una representación gráfica de los datos.	Exigido	
	El panel de informes debe proporcionar una vista rápida de los eventos de las últimas 24 horas.	Exigido	
	La solución debe permitir identificar fácilmente las actividades, las tendencias y los posibles ataques de la red.	Exigido	
	La solución deberá permitir realizar copias de seguridad de manera sencilla de los registros con recuperación rápida para las necesidades de auditoría.	Exigido	
	Implementación simplificada sin necesidad de conocimientos técnicos.	Exigido	
	La solución debe permitir crear informes personalizados con potentes herramientas de visualización.	Exigido	
	Búsqueda y visualización de Syslog.	Exigido	
	La solución debe permitir el almacenamiento de datos de Syslog en la consola de administración central.	Exigido	

	La consola debe permitir a los administradores crear informes bajo demanda.	Exigido	
	La solución debe de informar de nuevas aplicaciones en la nube (CASB).	Exigido	
	El equipo deberá ofrecer como característica el Servicio de correlacionador de eventos en el mismo dispositivo de forma embebida, sin incurrir en un costo adicional. El sistema reportería y correlacionamiento debe residir en el mismo appliance Firewall, no se permitirá una licencia adicional ni ningún equipo (Virtual, Hardware o Cloud) para lograr esta funcionalidad.	Exigido	
	Debe contar con informes integrados con opción de personalizar: paneles (tráfico, seguridad y cociente de amenazas del usuario), aplicaciones (riesgo de aplicaciones, aplicaciones bloqueadas, aplicaciones sincronizadas, motores de búsqueda, servidores web, coincidencia de palabras clave web, FTP), red y amenazas (IPS, ATP, inalámbrico, VPN, correo electrónico, cumplimiento (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)	Exigido	
	Monitoreo de actividad actual: estado del sistema, usuarios en vivo, conexiones IPSec, usuarios remotos, conexiones en vivo, clientes inalámbricos, cuarentena y ataques DoS.	Exigido	
	Programación de informes a varios destinatarios por grupo de informes con opciones de frecuencia flexibles.	Exigido	
	Capacidad de exportar informes como HTML, PDF, Excel (XLS).	Exigido	
	Personalización de la retención de registros por categoría	Exigido	
	Visor de registro en vivo con todas las funciones con vista de columna y vista detallada con potentes opciones de búsqueda y filtro, ID de regla con hipervínculo y personalización de la vista de datos	Exigido	
Cartas	Carta de Distribución del Representante / Distribuidor Local y del Fabricante de los Equipos Ofertados. Demostrar la cadena de autorizaciones desde el Fabricante hasta el Oferente con referenica al proceso.	Exigido	

	Catálogos y especificaciones del equipo ofertado.	Exigido	
Garantía	Garantía del Fabricante de 3 años	Exigido	
	Garantía de hardware y RMA con intercambio avanzado.	Exigido	
	Soporte 24x7 por teléfono y correo electrónico en inglés y Soporte 8x5 en español.	Exigido	
	Actualizaciones y parches de seguridad GRATIS.	Exigido	
	Actualizaciones y mejoras GRATUITAS de funciones de software	Exigido	
Se exigirá la presentación de	Certificado ISO 9001:2015 del fabricante	Exigido	
	Catálogos y especificaciones del equipo ofertado.	Exigido	
Componentes del equipo	Los componentes deberán contar con identificación original del fabricante. No se aceptarán partes que no sean originales del fabricante del Equipo.	Exigido	
	Adjuntar Listado de Componentes de manera a verificar en la Documentación Oficial del Fabricante el cumplimiento de las EETT.	Exigido	
Otras Características	El Firewall deberá incluir la funcionalidad y el licenciamiento para WAF y Email Protection por un periodo de 24 meses.	Exigido	
	Estas funcionalidades se deben lograr dentro del mismo appliance, no se permitirá firewall que no soporten estas funcionalidades a futuro o bien que requieran de algún appliance adicional (Virtual, Hardware o Cloud) para lograr dichas funcionalidades.	Exigido	
	Los Firewalls deberán contar con licencia mínima de 24 meses, la cual debe empezar a contabilizarse en tiempos, desde la entrega final de los equipos y su respectiva puesta en funcionamiento efectiva, no se aceptará que la licencia rija desde la compra de los mismos	Exigido	

3 - EQUIPO DE SEGURIDAD TIPO 2			
Descripción	**Descripción Técnica**	**Mínimo Exigido**	**Ofertado**
Cantidad:	13 (trece) unidades	Exigido	
Marca:	Especificar	Exigido	
Modelo:	Especificar	Exigido	
Procedencia:	Especificar		
Hardware	Procesador: Dos procesadores para diferentes fines, un procesador deber ser de tipo Flow Processor (NPU)	Exigido	
	RAM: 8 GB DDR4	Exigido	
	Almacenamiento integrado de al menos 64GB	Exigido	
	Puertos Ethernet: 9 Ethernet 10/100/1000/2500, SFPx1 puerto GBE SFP o superior	Exigido	
	Puertos de E/S: 1x USB 2.0, 1x COM (RJ45), 1x USB 3.0, 1 x Micro USB	Exigido	
	Fuente de alimentación: Auto-Ranging interno 110-240VAC, 50-60Hz	Exigido	
	Certificaciones de productos: CB, UL, CCC, CE, FCC	Exigido	
	Rendimiento del firewall: igual o superior a 15 Gbps	Exigido	
	Rendimiento del IPS: igual o superior a 3,5 Gbps	Exigido	
	Rendimiento de VPN IPsec: igual o superior a 12,5 Gbps	Exigido	
	Rendimiento de la protección contra amenazas: igual o superior a 3,25 Gbps	Exigido	

	Conexiones simultáneas: igual o superior a 4.900.000	Exigido	
	Nuevas conexiones/seg: igual o superior a 60,000	Exigido	
	Máximo de usuarios con licencia: sin restricciones	Exigido	
Características del firewall base	Interfaz accesible vía web con paneles configurables y segmentación de tráfico por categorías de aplicaciones.	Exigido	
	Gestión de reglas de firewall e interfaz de usuario optimizada y diseñada específicamente para grandes conjuntos de reglas de un vistazo e indicadores de cumplimiento.	Exigido	
	Soporte de autenticación en dos factores (contraseña única) para acceso de administrador, portal de usuario, IPSec y SSL VPN.	Exigido	
	Herramientas avanzadas de resolución de problemas en GUI (por ejemplo, captura de paquetes).	Exigido	
	Soporte de alta disponibilidad (HA) para agrupar dos dispositivos en modo activo-activo o activo-pasivo con configuración de HA rápida plug-and-play según sea requerido.	Exigido	
	Interfaz de línea de comandos completa (CLI) accesible desde la GUI.	Exigido	
	Administración basada en roles.	Exigido	
	Notificación de actualización de firmware automatizada con un sencillo proceso de actualización automática y funciones de reversión.	Exigido	
	Definiciones de objetos del sistema reutilizables para redes, servicios, hosts, períodos de tiempo, usuarios y grupos, clientes y servidores.	Exigido	
	Portal de usuarios de autoservicio.	Exigido	
	Seguimiento de cambios en configuración.	Exigido	

Control de acceso de dispositivos flexible para servicios por zonas.	Exigido	
Opciones de notificación por correo electrónico o SNMP.	Exigido	
Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.	Exigido	
Compatibilidad con SNMPv3 y Netflow.	Exigido	
Soporte de administración central a través de la consola unificada basada en la nube.	Exigido	
Notificaciones automáticas por correo electrónico para cualquier evento importante.	Exigido	
Configuraciones de copia de seguridad y restauración: localmente o correo electrónico; bajo demanda, diario, semanal o mensual.	Exigido	
API para integración de terceros.	Exigido	
Opción de acceso remoto para el soporte del Fabricante.	Exigido	
Gestión de licencias basada en la nube a través de un portal de licencias del Fabricante.	Exigido	
Soporte de Syslog.	Exigido	
Monitoreo de flujo en tiempo real.	Exigido	
Indicadores o Alertas de estilo semáforo.	Exigido	
Interacción rápida y detallada con cualquier widget del centro de control.	Exigido	
SNMP con una MIB personalizada y soporte para túneles VPN IPSec.	Exigido	
Soporte para nuevas instancias de AWS (C5 / M5 y T3)	Exigido	

	Soporte de zona WAN virtual en puertas de enlace personalizadas para el uso de un solo brazo posterior a la implementación.	Exigido	
Gestión de Firewall	La solución debe permitir la gestión de los equipos Firewall y los informes de estos equipos (hasta 7 días), desde una sola consola de gestión basada en la nube, donde, además, esta consola debe de proporcionar gestión de políticas por grupos de equipos.	Exigido	
	La gestión de políticas de grupo debe permitir que los objetos, la configuración y las políticas se modifiquen una vez y se sincronicen automáticamente con todos los Firewall del grupo.	Exigido	
	La consola debe proporcionar una pista de auditoría histórica completa y un seguimiento del estado de los cambios en las políticas del grupo.	Exigido	
	La consola además debe permitir la gestión de firmware de los equipos, así como el respaldo de los últimos cinco archivos de configuración para cada firewall.	Exigido	
	Las actualizaciones de firmware se deben ofrecen al administrador de la consola de tal manera que con un solo clic se pueda aplicar dicha actualización a cualquier dispositivo manejado dentro de la consola.	Exigido	
	La solución debe permitir implementaciones Zero-Touch desde esta consola central, permitiendo exportar la configuración para cargarla en un dispositivo desde una unidad flash, conectando así automáticamente al dispositivo a la consola Central.	Exigido	
	Debe permitir la programación de actualizaciones de firmware	Exigido	
	Debe permitir la generación de Informes de múltiples firewalls.	Exigido	
	Debe además permitir guardar, programar y exportar informes desde esta consola central.	Exigido	
	Esta Consola de gestión debe ser sin ningún costo	Exigido	

Firewall, Networking & Routing	El Firewall debe permitir una inspección profunda de paquetes donde todos paquetes deben ser inspeccionados por los motores de IPS, web, AV, control de aplicaciones e inspección SSL, utilizando un motor DPI (Deep Packet Inspection) de transmisión de alto rendimiento y sin proxy.	Exigido	
	El Firewall debe contar con Inspección TLS de alto rendimiento, debe contar con compatibilidad de TLS 1.3 sin degradación, políticas de nivel empresarial independientes del puerto, debe permitir una visibilidad única desde el panel de control así resolución de problemas de compatibilidad.	Exigido	
	El Firewall debe acelerar el tráfico de SaaS, SD-WAN y tráfico en la nube como: VoIP, video y otras aplicaciones confiables a través de	Exigido	
	El Firewall debe contar con una tecnología que le permita descargar el tráfico de forma inteligente para transferir el tráfico confiable a altas velocidades. La descarga de este tráfico se deberá controlar mediante una política para acelerar el tráfico importante de aplicaciones en la nube, o de forma inteligente en función de las características del tráfico.	Exigido	
	Debe contar con una lista de excepciones pre empaquetada.	Exigido	
	Debe cubrir todos los puertos / protocolos.	Exigido	
	Debe admitir todas las suites de cifrado modernas.	Exigido	
	La solución debe proporcionar políticas basadas en usuarios, grupos, horarios o redes.	Exigido	
	La solución debe proporcionar políticas de tiempo de acceso por usuario / grupo.	Exigido	
	La solución deberá hacer cumplir las políticas en zonas, redes o por tipo de servicio.	Exigido	
	La solución deberá contar con un firewall basado en zonas.	Exigido	
	Deberá proporcionar las zonas predeterminadas para LAN, WAN, DMZ, LOCAL, VPN y WiFi.	Exigido	

La solución deberá permitir el soporte completo de VLAN.	Exigido	
Deberá permitir el aislamiento de zonas y VLAN.	Exigido	
La solución deberá permitir la microsegmentación y autoaislamiento mediante seguridad sincronizada.	Exigido	
Deberá permitir personalizar zonas en LAN o DMZ.	Exigido	
La solución de Firewall deberá permitir la creación de políticas NAT personalizables con enmascaramiento de IP y soporte completo de objetos para redirigir o reenviar múltiples servicios en una sola regla con un asistente de reglas para crear rápida y fácilmente reglas NAT complejas con solo unos pocos clics.	Exigido	
La solución deberá contar con protección flood: bloqueo DoS, DDoS y escaneo de puertos.	Exigido	
Deberá permitir el bloqueo de país por geo-IP.	Exigido	
La solución deberá ofrecer enrutamiento avanzado: estático, multidifusión (PIM-SM) y dinámico (RIP, BGP, OSPF) con compatibilidad total con VLAN 802.1Q.	Exigido	
Deberá permitir el enrutamiento de multidifusión independiente del protocolo con snooping IGMP.	Exigido	
La solución deberá contar con soporte y etiquetado de VLAN DHCP.	Exigido	
La solución deberá contar con soporte Jumbo Frame.	Exigido	
La solución de Firewall deberá permitir el equilibrio de enlace SD-WAN: múltiples conexiones a Internet, verificación de estado de enlace automático, conmutación por error automática, equilibrio automático y ponderado y reglas granulares de múltiples rutas.	Exigido	
La solución deberá permitir la configuración completa de DNS, DHCP y NTP.	Exigido	

	Deberá permitir DNS dinámico (DDNS).	Exigido	
	Deberá contar con la certificación de aprobación del programa de logotipo IPv6 Ready.	Exigido	
	La solución deberá brindar soporte de tunelización IPv6 que incluye implementación rápida 6in4, 6to4, 4in6 e IPv6 (6rd) a través de IPSec.	Exigido	
SD-WAN	La solución deberá permitir el soporte para múltiples opciones de enlace WAN, incluyendo VDSL, DSL, cable y celular 3G / 4G / LTE con monitoreo esencial, balanceo, failover y fail-back".	Exigido	
	Selección de ruta de aplicación y enrutamiento, que se utiliza para garantizar la calidad y minimizar la latencia para aplicaciones de misión crítica como VoIP.	Exigido	
	SD-WAN sincronizada: La solución de firewall debe garantizar la integración con el Antivirus del mismo fabricante permitiendo sincronizar la seguridad de ambos componentes para así aprovechar la claridad y confiabilidad de la identificación de aplicaciones que viene con el intercambio de información entre los puntos finales administrados y el firewall.	Exigido	
	La solución deberá permitir el enrutamiento sincronizado de aplicaciones SD-WAN a través de enlaces preferidos a través de reglas de firewall o enrutamiento basado en políticas.	Exigido	
	Deberá permitir la implementación asequible, flexible y sin intervención o con poca intervención.	Exigido	
	Deberá contar con soporte VPN robusto que incluye IPSec y SSL VPN	Exigido	
	Deberá permitir la orquestación de VPN centralizada	Exigido	
	Integración con Azure Virtual WAN para una red de superposición SD-WAN completa	Exigido	
Cuotas y configuración de Traffic Shaping	La solución deberá permitir configurar "Traffic Shaping (QoS) en la red o basado en el usuario (con opciones mejoradas de tráfico web y de aplicaciones incluidas con la suscripción del mismo fabricante).	Exigido	

	Deberá permitir establecer cuotas de tráfico basadas en el usuario en carga / descarga o tráfico total y cíclico o no cíclico.	Exigido	
	Deberá permitir la optimización de VoIP en tiempo real.	Exigido	
Protección y Control Wireless	La solución deberá permitir una implementación simple plug-and-play de puntos de acceso inalámbricos (AP), que permita automáticamente aparezcan disponibles en el centro de control del firewall para su administración.	Exigido	
	Deberá permitir el alto rendimiento con el último estándar inalámbrico 802.11ac.	Exigido	
	Deberá contar con un monitoreo y administración centralizadas para los AP y clientes inalámbricos a través del controlador inalámbrico incorporado.	Exigido	
	Puente de AP a LAN, VLAN o una zona separada con opciones de aislamiento de clientes.	Exigido	
	Deberá poseer la compatibilidad con varios SSID por radio, incluidos los SSID ocultos.	Exigido	
	Deberá brindar soporte para los últimos estándares de seguridad y cifrado, incluidos WPA2 Personal y Enterprise.	Exigido	
	Deberá permitir la opción de selección de ancho de canal.	Exigido	
	Deberá permitir el soporte para IEEE 802.1X (autenticación RADIUS) con soporte para servidor primario y secundario.	Exigido	
	Deberá permitir el soporte para 802.11r (transición rápida).	Exigido	
	La solución deberá permitir la creación de cupones (personalizados), contraseña del día o aceptación de T&C.	Exigido	
	Deberá permitir el acceso a Internet de invitados con acceso a la red inalámbrica basada en el tiempo.	Exigido	

	La solución deberá permitir el modo de red en malla y repetición inalámbrica con Aps admitidos.	Exigido	
	Deberá optimizar la selección automática de canales.	Exigido	
	Deberá contar con soporte para inicio de sesión HTTPS.	Exigido	
	La solución deberá tener la capacidad de detección de puntos de acceso no autorizados.	Exigido	
Autenticación	La solución deberá permitir la autenticación a través de: Active Directory, eDirectory, RADIUS, LDAP y TACACS +.	Exigido	
	Deberá brindar agentes de autenticación para Active Directory, SSO.	Exigido	
	La solución deberá contar con un inicio de sesión único: Active Directory, eDirectory, RADIUS.	Exigido	
	La consola deberá permitir la autenticación de dos factores (2FA) y autenticación multifactor (MFA)	Exigido	
	Deberá permitir la compatibilidad con los agentes de autenticación de cliente para Windows, Mac OS X, Linux 32/64.	Exigido	
	Deberá contar con la autenticación SSO del navegador: autenticación de proxy transparente (NTLM) y Kerberos.	Exigido	
	Deberá brindar un portal cautivo de inicio de sesión en los navegadores.	Exigido	
	La solución deberá contar con certificados de autenticación para iOS y Android.	Exigido	
	Deberá permitir servicios de autenticación para IPSec, SSL como mínimo.	Exigido	
	Deberá contar con soporte de autenticación de Google Chromebook para entornos con Active Directory.	Exigido	
	Deberá contar con autenticación basada en API.	Exigido	

	Deberá soportar Integración con Azure AD.	Exigido	
	Soporte para crear usuarios con formato UPN para autenticación RADIUS.	Exigido	
Portal de Autoservicio de usuario	Los usuarios podrán descargar el cliente de autenticación desde la consola en la nube del mismo fabricante.	Exigido	
	Los usuarios a través de la consola central podrán descargar el cliente de acceso remoto SSL (Windows) y los archivos de configuración.	Exigido	
	El portal deberá permitir a los usuarios la opción de cambiar nombre de usuario y contraseña.	Exigido	
	El portal de autoservicio deberá permitir ver el uso personal de Internet.	Exigido	
	El portal deberá permitir acceder a mensajes en cuarentena y administrar listas de remitentes de bloqueo / permiso basadas en usuarios	Exigido	
Opciones de VPN	La solución de Firewall deberá permitir crear túneles VPN IPSec y SSL ilimitados.	Exigido	
	La solución de Firewall deberá permitir crear VPN de sitio a sitio: SSL, IPSec, PFS, RSA, certificados X.509, con clave previamente compartida.	Exigido	
	Soporte a protocolos VPN modernos y seguros (por ejemplo, IPsec, SSL/TLS), con opción de compatibilidad con protocolos heredados solo si es requerido por la entidad.	Exigido	
	Deberá permitir las VPN basada en rutas.	Exigido	
	Deberá permitir el acceso remoto con: SSL, IPsec, iPhone / iPad / Cisco / Soporte de cliente VPN de Android.	Exigido	
	Deberá brindar soporte al protocolo IKEv2 que se utiliza para negociar una asociación de seguridad al principio de una sesión.	Exigido	

	La solución deberá permitir a los usuarios la descarga del cliente SSL para Windows y la descarga de la configuración a través del portal de usuarios del mismo fabricante.	Exigido	
	La solución deberá permitir la aplicación de TLS 1.2 para túneles VPN de acceso remoto y sitio a sitio SSL.	Exigido	
Cliente IPSec	El cliente VPN deberá permitir el soporte de IPSec y SSL.	Exigido	
	El cliente de VPN deberá aprovisionarse e implementarse de una manera sencilla.	Exigido	
	La solución de Firewall deberá permitir el uso de licencias de acceso remoto SSL ilimitadas incluidas sin cargo adicional.	Exigido	
	Deberá contar con la autenticación: Clave pre compartida (PSK), PKI (X.509), Token y XAUTH.	Exigido	
	Deberá contar con un túnel dividido inteligente para un enrutamiento óptimo del tráfico.	Exigido	
	Deberá permitir el soporte NAT-transversal.	Exigido	
	El cliente VPN deberá permitir al cliente descripción gráfica del estado de la conexión.	Exigido	
	El cliente VPN deberá contar con soporte para sistema operativos Mac y Windows.	Exigido	
	Deberá contar con aprovisionamiento de políticas IPSec de acceso remoto con el cliente VPN del mismo fabricante.	Exigido	
	La solución deberá con soporte grupal para el cliente VPN del mismo fabricante que permita importaciones desde AD / LDAP, etc.	Exigido	
Prevención de Intrusiones	La solución deberá proveer un motor de inspección profunda de paquetes IPS de próxima generación y alto rendimiento con patrones IPS selectivos que se permitan aplicar sobre la base de una regla de firewall para obtener el máximo rendimiento y protección.	Exigido	

	La solución deberá proveer la protección contra amenazas de día cero.	Exigido	
	La solución deberá permitir el soporte para firmas IPS personalizadas.	Exigido	
	La solución deberá permitir filtros inteligentes de políticas IPS, esto permite a las políticas dinámicas actualizarse automáticamente a medida que se agregan nuevos patrones.	Exigido	
Protección ATP y Sincronización de los Sistemas de Seguridad	La solución deberá proveer la protección contra amenazas avanzada (detecta y bloquea el tráfico de red que intenta contactar con los servidores de comando y control mediante DNS de varias capas, AFC y firewall).	Exigido	
	La solución debe permitir integración con plataformas de endpoint protection (EPP/EDR) vía APIs estándar o mecanismos de interoperabilidad. Además, está sincronización deberá garantizar:	Exigido	
	Limitar el acceso a los recursos de red o aislar completamente los sistemas comprometidos hasta que se limpien.	Exigido	
	Prevenir los movimientos laterales y que aísle los sistemas comprometidos automáticamente en los puntos finales administrados por el antivirus.	Exigido	
VPN sin cliente	La solución deberá permitir a los usuarios acceder al portal de autoservicio HTML5 cifrado único con soporte para RDP, HTTP, HTTPS, SSH y VNC.	Exigido	
Características de protección web	La solución deberá proveer una protección completamente transparente para antimalware y filtrado web.	Exigido	
	La solución deberá contar con la protección avanzada contra amenazas mejorada.	Exigido	
	La solución deberá proveer una base de datos de filtrado de URL con millones de sitios en 92 categorías respaldados por OEMLabs o motores con capacidades equivalentes.	Exigido	

La solución deberá permitir configurar políticas de tiempo de cuota de navegación por usuario / grupo	Exigido	
La solución deberá permitir configurar políticas de tiempo de acceso por usuario / grupo	Exigido	
La solución deberá permitir configurar el escaneo de malware para bloquear todas las formas de virus, malware web, troyanos y spyware en HTTP / S, FTP y correo electrónico basado en la web.	Exigido	
Protección avanzada contra malware web con emulación de JavaScript.	Exigido	
Búsquedas en la nube en tiempo real para obtener la inteligencia de amenazas más reciente.	Exigido	
La solución de Firewall deberá proveer un segundo motor de detección de malware independiente para escaneo dual.	Exigido	
La solución deberá permitir el escaneo en tiempo real o en modo por lotes.	Exigido	
La solución deberá permitir configurar el escaneo HTTP y HTTPS por usuario o por política de red con reglas y excepciones personalizables.	Exigido	
La solución deberá permitir el almacenamiento en caché de contenido web de alto rendimiento.	Exigido	
Filtrado de tipo de archivo por tipo mime, extensión y tipos de contenido activo (por ejemplo, Activex, applets, cookies, etc.)	Exigido	
La solución deberá permitir configurar SafeSearch (basada en DNS) para los principales motores de búsqueda por política (usuario / grupo).	Exigido	
La solución deberá permitir el bloqueo de aplicaciones potencialmente no deseadas (PUA)	Exigido	

	La solución deberá permitir aplicar listas externas de categorización de contenido web para bloqueo automático de sitios ilegales, incluyendo listas globales reconocidas como IWF o equivalentes.	Exigido	
Visibilidad de Aplicaciones en la Nube	El Firewall deberá mostrar la cantidad de datos cargados y descargados en aplicaciones en la nube categorizadas como nuevas, autorizadas, no autorizadas o toleradas.	Exigido	
	La solución deberá permitir obtener detalles sobre usuarios, tráfico y datos de una manera profunda.	Exigido	
	La solución deberá permitir el acceso con un clic a las políticas de configuración del tráfico.	Exigido	
	La solución deberá permitir el filtro para el uso de aplicaciones en la nube por categoría o volumen	Exigido	
	La solución brindará un informe detallado y personalizable de uso de aplicaciones en la nube para informes históricos.	Exigido	
Protección y Control de Aplicaciones	La solución deberá permitir el control de aplicaciones para identificar, clasificar y controlar automáticamente todas las aplicaciones desconocidas de Windows y Mac en la red al compartir información entre los puntos finales y el firewall.	Exigido	
	La solución deberá permitir el control de aplicaciones basado en firmas con patrones para miles de aplicaciones.	Exigido	
	La solución brindará visibilidad y control de aplicaciones en la nube.	Exigido	
	La solución deberá permitir configurar filtros inteligentes de control de aplicaciones que habilitan políticas dinámicas que se actualizan automáticamente a medida que se agregan nuevos patrones.	Exigido	
	La solución deberá permitir configurar control de aplicaciones basado en categoría, características (por ejemplo, ancho de banda y consumo de productividad), tecnología (por ejemplo, P2P) y nivel de riesgo.	Exigido	

	La solución deberá permitir la aplicación de políticas de control de aplicaciones por reglas de usuario o de red.	Exigido	
	La solución debe garantizar la integración con Endpoints con el fin de identificar y sincronizar aplicaciones desconocidas que se estén ejecutando en la red permitiendo la administración y control de la misma. El firewall debe permitir al administrador cambiar el nombre y personalizar esas aplicaciones. Asignar aplicaciones a filtros de aplicaciones para controlar su tráfico.	Exigido	
Web & App Traffic Shaping	La solución deberá permitir configurar opciones personalizadas de Traffic Shaping (QoS) por categoría web o aplicación para limitar o garantizar la carga / descarga o la prioridad total del tráfico y la tasa de bits de forma individual o compartida.	Exigido	
Logging y Reportería	Informes predefinidos con opciones de personalización flexibles.	Exigido	
	Informes para firewalls desde un único punto central (hardware, software, virtual y en la nube hasta para 7 días.	Exigido	
	La interfaz de usuario deber ser intuitiva y proporcionar una representación gráfica de los datos.	Exigido	
	El panel de informes debe proporcionar una vista rápida de los eventos de las últimas 24 horas.	Exigido	
	La solución debe permitir identificar fácilmente las actividades, las tendencias y los posibles ataques de la red.	Exigido	
	La solución deberá permitir realizar copias de seguridad de manera sencilla de los registros con recuperación rápida para las necesidades de auditoría.	Exigido	
	Implementación simplificada sin necesidad de conocimientos técnicos.	Exigido	
	La solución debe permitir crear informes personalizados con potentes herramientas de visualización.	Exigido	
	Búsqueda y visualización de Syslog.	Exigido	

La solución debe permitir el almacenamiento de datos de Syslog en la consola de administración central.	Exigido	
La consola debe permitir a los administradores crear informes bajo demanda.	Exigido	
La solución debe de informar de nuevas aplicaciones en la nube (CASB).	Exigido	
El equipo deberá ofrecer como característica el Servicio de correlacionado de eventos en el mismo dispositivo de forma embebida, sin incurrir en un costo adicional. El sistema reportería y correlacionamiento debe residir en el mismo appliance Firewall, no se permitirá una licencia adicional ni ningún equipo (Virtual, Hardware o Cloud) para lograr esta funcionalidad.	Exigido	
Debe contar con informes integrados con opción de personalizar: paneles (tráfico, seguridad y cociente de amenazas del usuario), aplicaciones (riesgo de aplicaciones, aplicaciones bloqueadas, aplicaciones sincronizadas, motores de búsqueda, servidores web, coincidencia de palabras clave web, FTP), red y amenazas (IPS, ATP, inalámbrico, VPN, correo electrónico, cumplimiento (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)	Exigido	
Monitoreo de actividad actual: estado del sistema, usuarios en vivo, conexiones IPSec, usuarios remotos, conexiones en vivo, clientes inalámbricos, cuarentena y ataques DoS.	Exigido	
Programación de informes a varios destinatarios por grupo de informes con opciones de frecuencia flexibles.	Exigido	
Capacidad de exportar informes como HTML, PDF, Excel (XLS).	Exigido	
Personalización de la retención de registros por categoría	Exigido	
Visor de registro en vivo con todas las funciones con vista de columna y vista detallada con potentes opciones de búsqueda y filtro, ID de regla con hipervínculo y personalización de la vista de datos	Exigido	

Cartas	Carta de Distribución del Representante / Distribuidor Local y del Fabricante de los Equipos Ofertados. Demostrar la cadena de autorizaciones desde el Fabricante hasta el Oferente con referenica al proceso.	Exigido	
	Catálogos y especificaciones del equipo ofertado.	Exigido	
Garantía	Garantía del Fabricante de 3 años	Exigido	
	Garantía de hardware y RMA con intercambio avanzado.	Exigido	
	Soporte 24x7 por teléfono y correo electrónico en inglés y Soporte 8x5 en español.	Exigido	
	Actualizaciones y parches de seguridad GRATIS.	Exigido	
	Actualizaciones y mejoras GRATUITAS de funciones de software	Exigido	
Se exigirá la presentación de:	Certificado ISO 9001:2015 del fabricante	Exigido	
	Catálogos y especificaciones del equipo ofertado.	Exigido	
Otras Características	El Firewall deberá incluir la funcionalidad y el licenciamiento para WAF y Email Protection por un periodo de 24 meses.	Exigido	
	Estas funcionalidades se deben lograr dentro del mismo appliance, no se permitirá firewall que no soporten estas funcionalidades a futuro o bien que requieran de algún appliance adicional (Virtual, Hardware o Cloud) para lograr dichas funcionalidades.	Exigido	
	Los Firewalls deberán contar con licencia mínima de 24 meses, la cual debe empezar a contabilizarse en tiempos, desde la entrega final de los equipos y su respectiva puesta en funcionamiento efectiva, no se aceptará que la licencia rija desde la compra de los mismos	Exigido	

	La solución deberá integrarse nativamente con la consola de administración, permitiendo la gestión unificada de dispositivos, políticas, actualizaciones, reportes, alertas y licencias, sin requerir herramientas adicionales, migraciones de configuración ni costos extra por software de terceros. Este requisito se establece a fin de asegurar la continuidad tecnológica, optimizar la operación del entorno de seguridad, reducir la curva de aprendizaje del personal técnico, minimizar riesgos operativos y preservar las inversiones previamente realizadas por la Convocante.	Exigido	
Capacidad técnica del Oferente	El oferente deberá presentar al menos 2 personas certificadas en la marca ofertada de nivel ingeniero y/o arquitecto o equivalente	Exigido	
Instalación	Puesto en sitio, los equipos con instalación dentro del datacenter, configuración y todo lo necesario para su funcionamiento, instalados y mantenidos por dos años.	Exigido	

4 - SWITCH CORE			
Descripción	**Descripción Técnica**	**Mínimo Exigido**	**Ofertado**
Marca		Exigido	
Modelo		Exigido	
Procedencia		Exigido	
Cantidad	2 (dos) unidades	Exigido	
Descripción	Switch de 48 puertos	Exigido	
Interfaces			
Puertos para datos	- 48x puertos 1G/10G (SFP/SFP+)	Exigido	
	- 4x puertos 40G/100G (QSFP+/QSFP28)		

	El proveedor deberá incluir todo el licenciamiento que el equipo requiera para cumplir esta condición.		
Puertos para administración	- 1 puerto serial de consola RJ45	Exigido	
	- 1 puerto consola USB-C		
	- 1 puerto Ethernet RJ45 para administración fuera de banda.		
	- 1 USB para administración de archivos.		
Interfaces incluidas	Se deberá incluir:	Exigido	
	- 12 (doce) Transceivers de 10GE SFP+ duplex multimodo.		
Características generales y de rendimiento			
Formato	Rackeable 1U	Exigido	
Rendimiento	Switching 1.3 Tbps	Exigido	
	Throughput 1.000 Mpps	Exigido	
	No bloqueante	Exigido	
Sistema Operativo	El sistema operativo debe incluir el licenciamiento de todos los puertos y características de servicio mencionados en esta ficha. Los servicios especiales que requieran licenciamiento avanzado se deben mencionar expresamente.	Exigido	
Requerimientos L2			
Tamaño de tablas	- 147.000 direcciones MAC	Exigido	
VLANs	- 4000 VLAN Ids	Exigido	

Tramas	- Jumbo frames de 9K bytes	Exigido	
Spanning tree	- Spanning tree estándar IEEE 802.1D	Exigido	
	- Rapid STP IEEE 802.1w		
	- Multiple STP (MSTP) IEEE 802.1s		
	- Rapid Per-VLAN Spanning Tree (RPVST+)		
Características	- IEEE 802.1v para aislamiento automático en VLANs de protocolos no IPv4	Exigido	
	- VXLAN estáticos y dinámicos con BGP-EVPN		
	- ERPS (Ethernet Ring Protection Switching)		
	- MVRP		
	- Multichassis Link aggregation (capacidad de agregación de enlaces en todos los switches del cluster)		
	- IGMP para el manejo y control de multicast en capa 2		
	- Private VLAN (PVLAN)		
	- IEEE 802.3ad LACP, soporte de 52 grupos (cada grupo con soporte de hasta 8 enlaces)con selección del algoritmo de hashing L1-4		
	- LLDP		
	- QinQ		
Requerimientos L3			
Performance	- 24.500 rutas IPv4	Exigido	

	- 12.250 rutas IPv6		
Protocolos	- ECMP Equal-Cost Multipath	Exigido	
	- Rutas estáticas IPv4/IPv6		
	- RIPv2, RIPng		
	- OSPF, OSPFv2, OSPFv3		
	- BGP-4, MP-BGP		
	- Policy-based routing		
	- Dual Stack IPv4/IPv6		
	- NLB (Network Load Balancer)		
Características	- ARP: estático, gratituous ARP, proxy ARP	Exigido	
	- DNS: cliente, servidor		
	- DHCP: relay, server, cliente		
	- GRE (Generic Routing Encapsulation)		
Multicast			
Multicast Listener Discovery	MLD para IPv6, v1 y v2	Exigido	
Protocol Independent Multicast (PIM)	- IGMP Snooping	Exigido	
	- PIM SM (Sparse Mode)		
	- PIM SSM (Source-specific Multicast)		

	- PIM DM (Dense mode)		
	- PIM para IPv4 e IPv6		
	- MSDP (Multicast Service Discovery Protocol)		
Internet Group Management (IGMP)	IGMP v1, v2 y v3	Exigido	
QoS			
Encolamiento	Al menos:	Exigido	
	- Strict Priority		
	- Deficit WRR (DWRR)		
	- DCB (Data Center Bridging), DCB Exchange protocol, Priority Flow Control (PFC), Enhanced Transmission Service (ETS)		
	- Control de flujo para prevenir acumulación excesiva de congestion y evitar el packet buffering por periodos extensos.		
	- Soporte para servicios de almacenamiento: iSCSI, Lossless iSCSI, RDMA over Converged Ethernet version 2 (RoCE v1 and v2) y Non-Volatile Memory Express (NVMe over Fabrics)		
Servicio	Al menos:	Exigido	
	- 802.1p		
	- DSCP		
	- CoS		
	- IP SLA para monitoreo de degradación de varios servicios		

Seguridad			
Autenticación para administración	Soporte de:	Exigido	
	- Radius		
	- TACACS+		
	- RadSec		
Gestión segura	Acceso seguro a la gestión cifrando el tráfico (CLI, GUI, MIB) por medio de SSHv2, HTTPS, SNMPv3	Exigido	
Características	Al menos:	Exigido	
	- Listas de acceso de control (ACL) soportadas en IPv4 e IPv6. También protegen el plano de control SSH, SNMP, NTP o servidor web.		
	- Private VLAN (PVLAN)		
	- TPM (Trusted Platform Module) para asegurar la integridad de la plataforma		
	- Soporte de EST (Enrollment over Secure Transport) que permite el enrolamiento seguro de certificados, lo que permite una gestión más sencilla de PKI.		
	- Port security permite el acceso de direcciones MAC específicas, que pueden ser aprendidas o especificadas por el administrador		
	- MAC lockdown, también conocido como direccionamiento estático, se utiliza para evitar el movimiento de la estación y el secuestro de la dirección MAC, al permitir que una dirección MAC determinada use solo un puerto asignado en el conmutador.		
	- BPDU filter, permite controlar la participación del STP por puerto.		

	- BPDU Guard, cuando la protección BPDU está habilitada, las interfaces que reciben BPDU se desactivan.		
	- DHCP snooping, ayuda evitar problemas causados por servidores DHCP no autorizados		
	- Loop Protection, puede encontrar bucles en la capa 2 en puertos no taggeados, así como en VLAN etiquetadas y redes VXLAN.		
	- FIPS 140-2		
Control de tormentas	Protección contra tormentas de datos unicast, broadcast y multicast con umbrales definidos por el cliente.	Exigido	
Alta disponibilidad	Al menos:	Exigido	
	- Multichassis Link aggregation (capacidad de agregación de enlaces en todos los switches del cluster)		
	- Permitir una arquitectura distribuida y redundante mediante la implementación de dos switches y que cada switch mantenga un control independiente, pero que permita sincronizado durante las actualizaciones o fallas. También admitir actualizaciones durante la operación en vivo.		
	- Soporte de UDLD o equivalente (Uni-directional Link Detection) para monitorear la conectividad del enlace y apagar puertos en ambos extremos si se detecta tráfico unidireccional, evitando loops en redes basadas en STP		
	- BFD (Bidirectional Forward Detection)		
	- VRRP (Virtual Router Redundancy Protocol)		
	- Soporte de NLB (Microsoft Network Load Balancer) para aplicaciones de servidores		

	- Proporcionar imágenes flash duales de archivos independientes del sistema operativo primario y secundario.		
Gestión			
Administración	- Capacidad de administración CLI, GUI, Nube.	Exigido	
	- CLI estándar de industria con una estructura jerárquica para reducir el tiempo y los gastos de capacitación. Ofrece mayor productividad en entornos de múltiples proveedores		
	- Interfaz API REST integrada, programable y fácil de usar		
	- Aprovisionamiento de día cero		
	- sFlow (RFC 3176)		
	- IPFIX		
	- Restricción en comandos para configuraciones críticas, proporcionar múltiples niveles de privilegios con protección por contraseña, registro de acceso local y remoto por syslog.		
	- TACACS+ proporciona autorización de acceso administrativo		
	- SNMP (v2c/v3) , MIBs estándar y extensiones privadas		
	- TFTP, SFTP, SSH		
	- NTP		
	- Almacenamiento de múltiples archivos de configuración en memoria flash		

	- Port mirroring para tráfico saliente y entrante hacia puerto de monitoreo local o remoto; soportar hasta 4 grupos de mirror con número ilimitado de puertos por grupo.		
	- Soportar un motor que automáticamente monitorea y analiza eventos que pueden impactar en la salud de la red. Este debe estar ubicado en el mismo switch para hacer análisis y monitoreo de eventos de manera distribuida.		
Hardware y Energía			
Montaje	Debe traer todos los accesorios para montaje y operación en rack estándar de 19"	Exigido	
Alimentación eléctrica	Soporte al menos:	Exigido	
	- AC 100-127 VAC, AC 200-240 VAC.		
	- 50/60 Hz.		
Redundancia en fuente de poder	2 fuentes reemplazables en caliente.	Exigido	
Redundancia en ventilación	3 arreglos de ventiladores reemplazables en caliente.	Exigido	
Medio ambiente	Cumplir al menos:	Exigido	
	- RoHS		
Temperatura de operación	0°C a 40°C	Exigido	
Humedad de operación	15% a 95% non-condensing	Exigido	
Garantía y Soporte			
Garantía	Garantía directa del fabricante por tres (3) años.	Exigido	

Documentación			
Calificación tecnológica	Para garantizar la protección de inversión, alineación con las tendencias tecnológicas de la industria, soporte y vigencia tecnológica y estar preparados para los requerimientos futuros, los equipos de comunicación ofertados deben corresponder a una marca o fabricante que figure como líder en el cuadrante de Cuadrante Mágico Gartner para soluciones de acceso LAN Wired and Wireless durante al menos los últimos cinco años. Debe presentar el informe correspondiente a cada año.	Exigido	
Autorización del fabricante	El oferente deberá presentar una carta de autorización del fabricante para presentar oferta (la nota del fabricante deberá estar dirigida a la licitación de referencia).	Exigido	
Técnicos Certificados	El oferente deberá contar con al menos 1 (uno) técnico certificado por el fabricante de la marca ofertada (Certificación Técnica). No serán aceptadas credenciales de ventas o preventas.	Exigido	

5 - LICENCIAS ANTISPAM			
Descripción	**Descripción Técnica**	**Mínimo Exigido**	**Ofertado**
Marca			
Modelo			
Procedencia			
Cantidad	200 (doscientos) unidades		
Descripción	solución de seguridad avanzada para correo electrónico, gestionada desde una plataforma en la nube centralizada, diseñada para proteger organizaciones contra amenazas enviadas por email	Exigido	

Funcionalidades principales	- Phishing avanzado - Malware y ransomware - Ataques de suplantación (spoofing, impersonation) - URLs maliciosas - Archivos adjuntos peligrosos - Fraudes de tipo BEC (Business Email Compromise)	Exigido	
Administración centralizada	- Gestión completa desde Consola única y central - Políticas a nivel de dominio, grupo y usuario - Visibilidad y control desde una única consola de seguridad	Exigido	
Tipo de licenciamiento	Licenciamiento por usuario / buzón	Exigido	
Duración de licencias	- Suscripción por 24 meses - Gestión y activación desde una Consola única y central	Exigido	
Capacidad técnica del Oferente	El oferente deberá presentar al menos 2 personas certificadas en la marca ofertada de nivel ingeniero y/o arquitecto o equivalente	Exigido	
Instalación	Puesto en sitio, configuración y todo lo necesario para su funcionamiento, instalados y mantenidos por 24 meses.	Exigido	
Cartas	Carta de Distribución del Representante / Distribuidor Local y del Fabricante de los Equipos Ofertados. Demostrar la cadena de autorizaciones desde el Fabricante hasta el Oferente con referencia al proceso.	Exigido	

6 - LICENCIAS ENCRIPTACION DE DISPOSITIVOS			
Descripción	**Descripción Técnica**	**Mínimo Exigido**	**Ofertado**
Marca			
Modelo			
Cantidad	150 (ciento cincuenta) unidades		

Descripción	Herramienta que permita administrar de forma centralizada el cifrado completo de discos (BitLocker en Windows y FileVault en macOS) para proteger datos en caso de pérdida o robo de dispositivos.	Exigido	
Funcionalidades principales	- Gestión centralizada de BitLocker y FileVault - Despliegue rápido y remoto del cifrado - Recuperación de claves (Key Recovery) desde consola o portal de autoservicio Reportes de cumplimiento y estado de cifrado - Administración orientada al usuario Integración nativa con un Gestor único y central	Exigido	
Tipo de licenciamiento	- Licenciamiento por usuario (per user) - Un usuario puede proteger uno o varios dispositivos con una sola licencia - Cada licencia habilita el cifrado de los dispositivos asociados a ese usuario	Exigido	
Duración de licencias	- Suscripción por 24 meses - Gestión y activación desde una Consola única y central	Exigido	
Capacidad técnica del Oferente	El oferente deberá presentar al menos 2 personas certificadas en la marca ofertada de nivel ingeniero y/o arquitecto o equivalente	Exigido	
Instalación	Puesto en sitio, configuración y todo lo necesario para su funcionamiento, instalados y mantenidos por 24 meses.	Exigido	
Cartas	Carta de Distribución del Representante / Distribuidor Local y del Fabricante de los Equipos Ofertados. Demostrar la cadena de autorizaciones desde el Fabricante hasta el Oferente con referencia al proceso.	Exigido	

7 - LICENCIAS WINDOWS SERVER			
Descripción	**Descripción Técnica**	**Mínimo Exigido**	**Ofertado**
Marca			
Modelo			

Cantidad	8 (ocho) unidades		
Licencia	Windows Server Data Center 2025, Pack-16 (licencia por 16 núcleos de CPU)	Exigido	
Vigencia	Perpetua	Exigido	
Entregables	Los derechos de las licencias deberán estar a nombre de la **ANNP** utilizando su respectiva cuenta.	Exigido	

8 - LICENCIAS WINDOWS CAL			
Descripción	**Descripción Técnica**	**Mínimo Exigido**	**Ofertado**
Marca		Exigido	
Modelo		Exigido	
Cantidad	300 (trecientos) unidades	Exigido	
Licencia	CALs Dominio Windows, Per-User	Exigido	
Vigencia	Perpetua	Exigido	
Entregables	Los derechos de las licencias deberán estar a nombre de la **ANNP** utilizando su respectiva cuenta.	Exigido	

9 - SERVICIO DE IMPLEMENTACION Y SOPORTE			
Descripción	**Descripción Técnica**	**Mínimo Exigido**	**Ofertado**
Descripción	Implementación y Soporte Técnico	Exigido	

Mantenimiento y soporte técnico a Next Generation Firewall	Mantenimiento Preventivo general del Hardware.	Exigido	
	Soporte técnico del oferente de la empresa adjudicada en modalidad de respuesta 8x5 por siguiente día hábil.		
	Entrega de documentación referente al estado de reglas y diagramas de configuración.		
	Actualización de versión de Software del Firewall Firmware		
	Soporte técnico para gestión de direcciones de red direcciones ip, interfaces, rutas y vpn.		
	Soporte técnico para problemas monitoreo y performance del UTM.		
	Soporte técnico para reportes de estados de enlaces y amenazas.		
	Revisión General e Informe de:		
	* Políticas de seguridad.		
	* Revisión de Seguridad Positiva / Negativa.		
	* Prueba de Penetración Semestral. El proveedor deberá realizar una evaluación de seguridad técnica (pentest) con periodicidad mínima semestral sobre la infraestructura implementada en el marco del presente contrato. La evaluación deberá: (a) seguir la metodología PTES, NIST SP 800-115 u otra similar reconocida; (b) cubrir como mínimo el perímetro de red, accesos VPN y consola de administración; (c) producir un informe con hallazgos clasificados por severidad (CVSS v3.1 o superior); (d) incluir plazos de remediación: vulnerabilidades críticas ≤ 15 días, altas ≤ 30 días, medias ≤ 90 días desde la entrega del informe.		
	Reglas de seguridad y nat de los equipos de seguridad		
	Revisión el diagrama lógico de red, además del diagrama físico de conexiones		

	Revisión de Tráfico en ambiente productivo		
	Revisión de la Gestión Unificada de Amenazas funcionalidades tales como: UDP, VPN, Antispam, Antiphishing, Antispyware, Filtro de contenidos, Antivirus, Detección/Prevención de Intrusos (IDS/IPS)		
	La empresa Oferente deberá contar con las siguientes certificaciones:		
	* Al menos 2 técnicos de nivel superior en soluciones de Networking. Ej.: CISCO CCNP, FORTINET NSE8.		
	* Al menos 4 técnicos de nivel medio en soluciones de Networking. Ej.: CISCO CCNA, FORTINET NSE4.		
	* Todo el personal técnico solicitado en este ítem deberá ser empleados de la empresa oferente con una antigüedad mínima de 24 meses, para demostrar este requerimiento serán aceptados la documentación que acredite la inclusión del profesional técnico al IPS.		
	El personal técnico deberá contar con documentación paraguaya.		
Soporte técnico equipamiento de networking.	Mantenimiento Preventivo general de Hardware	Exigido	
	Entrega de documentación referente al estado de reglas y diagramas de configuración		
	Actualización de versión de Software Firmware.		
	Configurar nuevas VLan para cualquier nueva estructura de Red a ser instaladas.		
	Configuración y Administración de segmentos de las redes.		
	Configuración de Accesos AAA (Autorización, Autenticación, Aucaunting)		
	Entrega de documentación referente al estado de reglas y diagramas de configuración nueva.		

	Soporte y asistencia técnica en caso de problemas físicos del cableado de backbone óptico.		
	La empresa Oferente deberá contar con las siguientes certificaciones:		
	* Al menos 2 Técnicos en Diseño e Implementación de cableado estructurado en redes LAN y Fibra óptica.		
	* Todo el personal técnico solicitado en este ítem deberá ser empleado de la empresa oferente con una antigüedad mínima de doce meses. Para demostrar este requerimiento serán aceptados la documentación que acredite la inclusión del profesional técnico al IPS.		
	* El personal técnico deberá contar con documentación paraguaya.		
Gestión continua durante el período de soporte	El proveedor aplicará actualizaciones de seguridad dentro de los plazos siguientes desde su publicación por el fabricante: vulnerabilidades críticas en ≤ 15 días calendario; vulnerabilidades altas en ≤ 30 días calendario. Todo cambio de configuración deberá registrarse con fecha, responsable y descripción del cambio	Exigido	

CONDICIONES GENERALES

- El Oferente Adjudicado deberá instalar y poner en funcionamiento todos los equipos y sistemas suministrados. Deberá contemplar en su oferta todos los materiales, accesorios, cables, licencias y servicios de manera a garantizar la correcta instalación e integración de la solución de acuerdo con lo requerido en las Especificaciones Técnicas.
- Se requiere que los equipos estén debidamente embalados, con todos sus accesorios y protegidos contra golpes al momento de la entrega.
- Soporte Técnico de los bienes ofertados, con posibilidad de escalamiento hasta el fabricante, previéndose las revisiones periódicas que resulten de la recomendación del fabricante, por el término de 24 (veinticuatro) meses contados a partir de la conformidad de estos emitida por el área administradora del Contrato.
- La adquisición incluirá los siguientes aspectos: Provisión, Instalación, Puesta en funcionamiento, Garantía, Servicio Técnico.
- El proveedor deberá incluir en su oferta el entrenamiento para el personal designado por la institución, con el fin de asegurar el correcto uso y manejo de los equipos adquiridos. El entrenamiento debe incluir todos los aspectos relevantes del uso de los Equipos.
- **Prueba de Aceptación de Seguridad**

  Como condición previa a la recepción provisional y puesta en producción, el proveedor deberá ejecutar una prueba de aceptación técnica de seguridad sobre la solución implementada.

  La validación deberá incluir, como mínimo:

  a) Verificación del hardening aplicado conforme a las recomendaciones del fabricante o estándares reconocidos.

  b) Revisión y validación de reglas de firewall, VPN, NAT y políticas de seguridad implementadas.

  c) Verificación del funcionamiento de los mecanismos de registro y auditoría (logs), así como su correcta generación y disponibilidad para análisis.

d) Validación de los mecanismos de autenticación administrativa, incluyendo controles de acceso y autenticación cuando corresponda.

e) Verificación operacional de las funcionalidades contratadas de seguridad, monitoreo y protección.

El proveedor deberá entregar un informe de aceptación técnica que documente las pruebas realizadas, los resultados obtenidos, las configuraciones aplicadas y las evidencias correspondientes. La recepción provisional quedará condicionada a la aprobación de dicho informe por parte de la convocante.

- **Revocación de Accesos del Proveedor**

Como condición previa a la recepción definitiva de la solución, el proveedor deberá proceder a la revocación o transferencia controlada de todos los accesos administrativos utilizados durante la implementación, configuración y puesta en producción de la infraestructura.

Como mínimo se deberá:

a) Eliminar o deshabilitar cuentas administrativas temporales creadas para el proyecto.

b) Transferir a la convocante la administración exclusiva de las credenciales privilegiadas.

c) Revocar certificados, claves o accesos remotos utilizados por personal del proveedor que no formen parte de los servicios de soporte contratados.

d) Documentar los mecanismos de acceso administrativo que permanecerán habilitados durante la vigencia del soporte.

- **Acuerdo de Nivel de Servicio (SLA) para soporte y ciberseguridad**

El proveedor deberá garantizar la prestación del servicio de soporte técnico especializado durante toda la vigencia contractual, estableciendo como mínimo los siguientes niveles de servicio:

Severidad	Descripción
Crítica (Sev-1)	Indisponibilidad total del firewall, clúster HA, VPN institucional, consola de administración, servicio MDR o incidente de seguridad con impacto significativo sobre los servicios de la convocante.
Alta (Sev-2)	Degradación significativa de los servicios de seguridad sin interrupción total de la operación.
Media (Sev-3)	Incidentes con impacto limitado o que disponen de mecanismos alternativos de operación.
Baja (Sev-4)	Consultas técnicas, requerimientos de cambios menores o incidencias sin impacto operativo relevante.

El adjudicado deberá garantizar como mínimo:

Severidad	Tiempo de respuesta inicial	Tiempo de escalamiento	Tiempo máximo de mitigación
Crítica (Sev-1)	≤ 1 hora	≤ 2 horas	≤ 4 horas

Alta (Sev-2)	≤ 4 horas	≤ 8 horas	≤ 24 horas
Media (Sev-3)	≤ 1 día hábil	≤ 2 días hábiles	≤ 5 días hábiles
Baja (Sev-4)	≤ 2 días hábiles	Según planificación de la ANNP	Según planificación de la ANNP

Adicionalmente:

a) El proveedor deberá mantener una mesa de ayuda para recepción y seguimiento de incidentes.

b) Todos los incidentes deberán contar con número de ticket y trazabilidad completa de atención.

c) Los incidentes relacionados con compromisos de seguridad, amenazas activas, malware, ransomware, indisponibilidad de firewall, interrupción de VPN o caída de servicios críticos deberán ser atendidos bajo esquema prioritario.

d) El proveedor deberá emitir informes mensuales de cumplimiento de SLA indicando cantidad de incidentes recibidos, tiempos de respuesta, tiempos de resolución y porcentaje de cumplimiento.

- **Configuraciones seguras iniciales**

  Antes de la puesta en producción de cada componente, el proveedor deberá aplicar una configuración segura documentada alineada al CIS Benchmark vigente del producto ofertado o, en su ausencia, a la guía de hardening oficial del fabricante, dicha configuración deberá:

  a) Eliminar o deshabilitar todas las cuentas y contraseñas de fábrica no estrictamente requeridas para la operación, reemplazándolas por credenciales de complejidad documentada.

  b) Deshabilitar todos los servicios, puertos y protocolos innecesarios. Quedan expresamente prohibidos en producción: Telnet, FTP, SNMPv1/v2c, SSLv2/v3, TLS 1.0/1.1 y cualquier interfaz de gestión en texto plano. Los reemplazos exigidos son SSH v2, SNMPv3 con autenticación SHA y cifrado AES, y TLS 1.2 como mínimo.

  c) Requerir autenticación multifactor (MFA) para todo acceso administrativo a consolas de gestión, interfaces web y accesos remotos.

  d) Configurar roles diferenciados con el mínimo privilegio necesario: al menos administrador, operador de monitoreo y auditor, sin privilegios administrativos en cuentas de uso general.

  e) Habilitar el registro de auditoría (logging) de accesos, cambios de configuración y eventos de seguridad desde el primer día de operación, con envío al sistema de monitoreo centralizado de la convocante.

- **Entregable obligatorio**

  Como condición previa a la recepción provisional, el proveedor entregará por cada componente un Informe de Cumplimiento de Configuración Segura que contenga: la guía de referencia aplicada con su versión, el listado de controles verificados con su estado de cumplimiento, las excepciones con su justificación técnica y el control compensatorio aplicado, y el inventario de cuentas y servicios activos al momento de la entrega. La convocante podrá verificar su contenido mediante inspección técnica directa.

De las MIPYMES

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

Plan de entrega de los bienes

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

Ítem	Descripción del bien	Cantidad	Unidad de medida	Lugar de entrega de los bienes	Fecha(s) final(es) de entrega de los bienes
1 al 9	*Adquisición e instalación de equipos de seguridad Firewall, llave en mano.*	*1*	*Unidad*	*GERENCIA DE UTIC Terminal Portuaria de Asunción*	*Dentro de los 70 días calendarios posteriores a la firma del contrato*

Plan de prestación de los servicios

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

No Aplica

Planos y diseños

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

No Aplica

Embalajes y documentos

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

No Aplica

1. El Proveedor embalará los bienes en la forma necesaria para impedir que se dañen o deterioren durante el transporte al lugar de destino final indicado en el contrato. El embalaje deberá ser adecuado para resistir, sin limitaciones, su manipulación brusca y descuidada, su exposición a temperaturas extremas, la sal y las precipitaciones, y su almacenamiento en espacios abiertos. En el tamaño y peso de los embalajes se tendrá en cuenta, cuando corresponda, la lejanía del lugar de destino final de los bienes y la carencia de equipo pesado de carga y descarga en todos los puntos en que los bienes deban transbordarse.

2. El embalaje, las identificaciones y los documentos que se coloquen dentro y fuera de los bultos deberán cumplir estrictamente con los requisitos especiales que se hayan estipulado expresamente en el contrato y cualquier otro requisito si lo hubiere, especificado en las condiciones contractuales.

Inspecciones y pruebas

Las inspecciones y pruebas serán como se indica a continuación:

No Aplica

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 indicado 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.

CONDICIONES CONTRACTUALES

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

Interpretación

1. Si el contexto así lo requiere, el singular significa plural y viceversa; y día significa día corrido, salvo que se haya indicado expresamente que se trata de días hábiles.

2. Condiciones prohibidas, inválidas o inejecutables. Si cualquier provisión o condición del contrato es prohibida o resultase inválida o inejecutable, dicha prohibición, invalidez o falta de ejecución no afectará la validez o el cumplimiento de las otras provisiones o condiciones del contrato.

Formalización de la Contratación

La convocante formalizará la contratación mediante: Contrato.

Documentación electrónica

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

Documentación requerida para la firma del contrato

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

1. Personas Físicas / Jurídicas

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

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

2. Documentos. Consorcios

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

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

En caso de consorcio en formación, el mismo deberá actualizar el RUC definitivo del consorcio constituido a través del Registro de Proveedores del Estado, previo a la comunicación del contrato y emisión del código de contratación.

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

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.

Confidencialidad en el procedimiento de contratación y el contrato.

La contratante y el proveedor deberán mantener confidencialidad y en ningún momento divulgarán a terceros, sin el

consentimiento de la otra parte, documentos, datos u otra información que hubiera sido directa o indirectamente proporcionada por la otra parte en conexión con el contrato, antes, durante o después de la ejecución del mismo.

Cuando dicha información incluya datos personales de personas físicas, las partes se obligan a realizar su tratamiento en estricto cumplimiento de la Ley N° 7593/2025 “De Protección de Datos Personales”, su reglamentación y demás normas aplicables, respetando en particular los principios de licitud, finalidad, minimización, confidencialidad, seguridad y diligencia debida, y limitando el tratamiento exclusivamente a los fines vinculados con la ejecución del contrato.

No obstante, el proveedor podrá proporcionar a sus subcontratistas los documentos, datos e información recibidos de la contratante para que puedan cumplir con su trabajo en virtud del contrato. En tal caso, el proveedor obtendrá de dichos subcontratistas un compromiso de confidencialidad similar al requerido al proveedor en la presente cláusula.

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

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

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

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

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

Porcentaje de Garantía de Fiel Cumplimiento de Contrato

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

10,00 %

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

Forma de Instrumentación de Garantía de Fiel Cumplimiento de Contrato

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

Condiciones especiales de la Garantía de Fiel Cumplimiento de Contrato

Las condiciones especiales de la Garantía de Fiel Cumplimiento de Contrato serán:

No Aplica

Periodo de validez de la Garantía de Cumplimiento de Contrato

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

12 meses contados A PARTIR DE LA SUSCRIPCION DEL CONTRATO

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

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

Solicitud de Pago de Anticipo

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

No Aplica

1. El anticipo es la suma de dinero que se entrega al proveedor, consultor o contratista destinada al financiamiento de los costos en que éste debe incurrir para iniciar la ejecución del objeto contractual. El mismo no constituye un pago por adelantado; debe estar amparado con una garantía correspondiente al cien por ciento de su valor y deberá ser amortizado durante la ejecución del contrato y durante la ejecución de contrato demostrar el debido uso. La Garantía de Anticipo deberá estar vigente desde la solicitud de pago del anticipo, y mantener su vigencia hasta su total amortización.

Los recursos entregados en calidad de anticipo no podrán destinarse a fines distintos a los relacionados con el objeto del contrato.

El proveedor, consultor o contratista que reciba pagos en concepto de anticipo estará obligado a informar a la contratante sobre el destino y la forma de aplicación del mismo, que en todos los casos estará relacionado al efectivo cumplimiento del contrato.

En caso de extensión de la Garantía de Anticipo, la misma deberá cubrir el saldo pendiente de amortización.

2. Si se establece en el SICP el otorgamiento de anticipos, no podrá superar en ningún caso el porcentaje establecido en la legislación vigente.

3. La solicitud de pago del anticipo deberá ser presentada por escrito, con la factura, el plan de inversiones y la Garantía de Anticipo.

4. El proveedor podrá remitir una comunicación por escrito a la contratante, en la cual informe que rechaza el anticipo previsto en el PBC. La falta de solicitud de anticipo en el plazo previsto en el PBC será considerada como un rechazo del mismo. En estos casos podrá darse inicio al cómputo de la ejecución contractual en las condiciones establecidas en el pliego de bases y condiciones.

5. El Pago del Anticipo debe ser total. En el caso que se realizare el pago de un porcentaje inferior al 100% del mismo, el proveedor podrá rechazarlo en el plazo de cinco (5) días hábiles mediante una nota de reclamo remitida a la Contratante. Transcurrido dicho

plazo, se considerará que el Anticipo ha sido aceptado por el proveedor y podrá darse inicio al cronograma de ejecución contractual en las condiciones establecidas en el pliego de bases y condiciones.

6. En el caso de que el proveedor haya solicitado el anticipo en las condiciones establecidas en la presente clausula y la convocante no ha procedido al pago, el oferente no está obligado a iniciar la ejecución del contrato hasta tanto el pago se haya efectuado de forma total o de acuerdo a lo dispuesto en el punto 5.

7. El proveedor deberá usar el anticipo únicamente para pagar costos que se requieran específicamente para la ejecución del contrato respectivo. El proveedor deberá informar a la contratante sobre el destino y la forma de aplicación del mismo y demostrar que ha utilizado el anticipo para gastos relacionados al efectivo cumplimiento del contrato mediante la presentación de copias de las facturas u otros documentos al administrador del contrato, quien junto con la contratante realizará el seguimiento y control de los recursos entregados. El proveedor estará obligado a proporcionar a la contratante los comprobantes y cualquier otra información que le fuera requerida con el objeto de comprobar el cumplimiento del plan de inversión del anticipo.

8. La amortización del anticipo se realizará de acuerdo con lo establecido en el contrato, en la proporción que éste indique.

9. Para la ejecución de esta garantía, especialmente cuando sea instrumentada a través de Póliza de Seguro de caución, será requisito que previamente el proveedor sea notificado del incumplimiento y la intimación de que se hará efectiva la ejecución del monto asegurado.

10. A menos que se indique otra cosa en este apartado, la Garantía de Anticipo será liberada por la contratante y devuelta al proveedor, a requerimiento de parte, a más tardar treinta (30) días contados a partir de la fecha de cumplimiento de las obligaciones del proveedor en virtud del contrato, pudiendo ajustarse por el saldo adeudado.

11. En el caso de rescisión o terminación anticipada del contrato, los proveedores o contratistas deberán reintegrar a la contratante el saldo por amortizar.

Forma de Instrumentación de Garantía de anticipo

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

No Aplica

Disponibilidad de créditos presupuestarios

El alcance de los compromisos asumidos, así como la provisión de los bienes y servicios acordados, quedarán supeditados durante su ejecución, a la efectiva disponibilidad de los créditos presupuestarios y de los planes financieros aprobados para el Ejercicio Fiscal vigente y en los ejercicios fiscales siguientes.

La Entidad contratante debe comunicar formalmente al proveedor la existencia del CDP correspondiente al ejercicio fiscal vigente.

En ausencia del CDP y de su comunicación expresa al proveedor, este quedará eximido de realizar la provisión de bienes y/o servicios, sin que dicha abstención genere responsabilidad alguna ni constituya causal de incumplimiento contractual, aun cuando se hubiera emitido la orden de ejecución.

En ningún caso serán admitidas como deudas del ejercicio fiscal vigente ni dará derecho a reclamación de pago alguno, la provisión de bienes o prestaciones de servicios que se efectuaren sin contar con la disponibilidad de los créditos presupuestarios correspondientes.

Indicadores de Cumplimiento de Contrato

El documento requerido para acreditar el cumplimiento contractual, será:

Planificación de indicadores de cumplimiento:

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA *(se indica la fecha que debe presentar según el PBC)*
Nota de Remisión / Acta de recepción 1	*Nota de Remisión / Acta de recepción*	*DICIEMBRE 2026*

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

Subcontratación

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

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

---

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

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

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

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

4. La contratante podrá realizar las diligencias que considere necesarias para verificar que la totalidad de las personas que

prestan servicios personales en relación de dependencia para la contratista y eventuales subcontratistas se encuentren debidamente individualizados en los listados recibidos.

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

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

Formas y condiciones de pago

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

1. Documentos Genéricos:

a. Nota de remisión u orden de prestación de servicios según el objeto de la contratación;

b. La factura de pago, con timbrado vigente, la cual deberán expresar claramente por separado el Impuesto al Valor Agregado (IVA) de conformidad con las disposiciones tributarias aplicables. En ningún caso el valor total facturado podrá exceder el valor adjudicado o las adendas aprobadas;

c. REPSE (registro de prestadores de servicios) todos los que son prestadores de servicios;

d. Certificado de Cumplimiento Tributario;

e. Constancia de Cumplimiento con la Seguridad Social;

f. Formulario de Identificación de Servicios Personales (FIS);

g. Certificado laboral vigente expedido por la Dirección de Obrero Patronal dependiente del Viceministerio de Trabajo, siempre que el sujeto esté obligado a contar con el mismo, de conformidad a la reglamentación pertinente - CPS

2.Documentos Específicos a la presente convocatoria:

- El reporte de la carga de la nómina del personal en el FIP, asignado a los servicios contratados o la actualización en su caso;
- La Declaración Jurada del Salario expedida por el Instituto de Previsión Social a fin de corroborar el cumplimiento efectivo de las cargas sociales;
- El extracto de las acreditaciones de pago de salarios al personal asignado, realizadas a través de Red Bancaria;
- Planilla de marcación de entrada y salida de los empleados de la empresa a la institución contratante.

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

Los pagos se realizaran dentro de los 30 días hábiles posteriores de la presentación de la factura correspondiente, previa conformidad por la entrega de los bienes/servicios por parte del Administrador del contrato. La solicitud deberá ser presentada mediante una Nota dirigida al Ing. Julio Cesar Vera Presidente del Directorio de la ANNP, a través de Mesa de Entrada de la Institución.

La factura deberá estar acompañada de los siguientes documentos:

- Las documentaciones citadas en el Punto - Formas y Condiciones de Pago (Documentos Genéricos)
- El ACTA DE RECEPCION DE LOS BIENES

Para el presente procedimiento NO APLICA la presentacion de los documentos Especificos requeridos para el pago correspondiente.

La Convocante no procesará los pagos que no contare con las documentaciones mencionadas.

Los pagos se realizarán conforme las disponibilidades del Plan Financiero Institucional y el plan de Caja y los fondos de la Contratante.

Las deducciones que se realizarán sobre las facturas serán:

- Contribución al sistema de contrataciones públicas 0,4% .
- Retenciones de IVA y Renta.
- Multas por atrasos en ejecución del cronograma de ejecución mensual por causa imputable al contratista. (si hubiere).

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

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

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

Anticipo MIPYMES

Se otorgará Anticipo MIPYMES:

No Aplica

Reajuste

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

El precio de los bienes se reajustaran durante el periodo de ejecución del contrato, a partir de una variación significativa de precios ocurrida en la economía nacional, que será medida a través del índice de precios al consumo, publicado por el Banco Central del Paraguay, en una relación porcentual igual o mayor al 15 % del mencionado índice acumulado a partir de la fecha de apertura de ofertas. Los ajustes deberán corresponder al periodo o mes de entrega de los bienes y aplicados sobre el importe facturado y presentado para su pago. El importe del precio ajustado de los bienes facturados debe corresponder a la siguiente formula:

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

Donde:

Pr: Precio Reajustado

P: Precio adjudicado

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

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

No reconocerá reajuste de precio si el suministro se encuentra atrasado respecto al cronograma de entrega

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, cuando la variación sea positiva, para cuya obtención se deberá cumplir con los requerimientos establecidos por la DNCP.

La aplicación de la formula deberá prever la deducción del anticipo financiero, en caso de haber sido otorgado. En caso que los índices oficiales que se deben utilizar en el cálculo no estén disponibles, se podrán efectuar ajustes provisionales utilizando los últimos índices conocidos. Los ajustes se corregirán cuando se conozcan los valores relativos a los meses en cuestión.

El coeficiente de ajuste se redondea a la millonésima superior.

El pago del reajuste se efectuará únicamente después de la emisión del acto administrativo que autoriza el precio reajustado y del correspondiente código de contratación.

Los reajustes de precios se aplicarán bajo solicitud expresa por parte del proveedor, conforme a la forma y plazo establecida en la normativa. El Administrador del Contrato es responsable de velar por la aplicación del reajuste de precios en caso de ser favorable a la Contratante.

Porcentaje de multas

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

0,40 %

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:

0,20

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

La mora será computada a partir del día siguiente del vencimiento del plazo de 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 correspondientes, 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 solicitar la suspensión del contrato, por motivos que no le serán imputables, de acuerdo a lo establecido en el artículo 66 de la Ley N° 7021/22.

La contratante, en virtud de causas establecidas en el contrato, está facultada para suspender la tramitación de un pago, en tal caso, las sumas correspondientes durante los atrasos resultantes no devengarán intereses por mora.

Pago de interés por mora.

Procedimiento para el pago de interés por mora:

En caso de que la Contratante incurriera en mora en el pago al Proveedor, el mismo podrá presentar la solicitud de reconocimiento de intereses moratorios por Mesa de Entrada de la ANNP, identificando el número de expediente de ingreso a la ANNP de la solicitud de pago de la factura pendiente de pago. Previa verificación de los antecedentes, la ANNP se expedirá respecto a la solicitud en un plazo de 15 (quince) días hábiles a ser contados desde el día siguiente a la fecha de presentación del requerimiento

---

Caso Fortuito o Fuerza mayor

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

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, embargos de cargamentos, explosiones, guerras, insurrección, movilización, huelgas, temblores de tierras y decisiones gubernamentales.
2. Para fines de esta cláusula, “Caso Fortuito” significa un evento extraordinario, imprevisto, inevitable, que imposibilita absolutamente el cumplimiento de la prestación y/u obligación. Cuando la previsión humana pueda anticipar el caso fortuito, el proveedor deberá acreditar haber empleado todos los recursos a su alcance para evitarlo y no se debe atribuir a la culpa o negligencia del mismo. Se debe tratar de un hecho externo al proveedor.
3. El proveedor deberá demostrar el nexo existente entre el caso notorio y la obligación pendiente de cumplimiento. El caso fortuito o la fuerza mayor solamente podrá afectar a la parte del contrato cuyo cumplimiento imposible fue demostrado.
4. Por consiguiente, no se considerarán como casos fortuitos o de Fuerza Mayor los actos o acontecimientos cuya ocurrencia podría preverse y cuyas consecuencias podrían evitarse actuando con diligencia razonable. De la misma manera, no se considerarán caso fortuito o fuerza mayor los actos o acontecimientos que hagan el cumplimiento de una obligación únicamente más difícil o más onerosa para la parte correspondiente.
5. Si se produjera un acontecimiento de Caso fortuito o fuerza mayor, el proveedor tendrá derecho a una prorroga razonable de los plazos de ejecución.
6. La parte que invoque fuerza mayor o caso fortuito deberá enviar una notificación sobre el caso a la otra parte, inmediatamente después que el acontecimiento sucedió y dentro del plazo máximo de siete (7) días calendarios a partir del día siguiente en que haya tenido conocimiento del evento o debiera haber tenido conocimiento del evento.
7. La notificación se enviará por nota o correo electrónico, estableciendo los elementos constitutivos del caso fortuito o la fuerza mayor y sus consecuencias probables para la ejecución del contrato, adjuntando toda la documentación comprobatoria. En todo caso, la parte afectada deberá tomar todas las medidas necesarias para conseguir, en el

menor plazo posible, la reanudación normal de la ejecución de las obligaciones afectadas por el caso fortuito o fuerza mayor.

8. Cuando la parte que invoque el caso fortuito o la fuerza mayor sea el contratista, y esta no haya notificado a la convocante la situación que le impide cumplir con las condiciones contractuales, no podrá invocar caso fortuito o fuerza mayor. Excepcionalmente, la convocante bajo su responsabilidad, podrá aceptar la notificación del evento de caso fortuito o de fuerza mayor cuando el atraso de la comunicación se deba a causas no imputables al proveedor, debiendo el administrador del contrato emitir un dictamen fundado aceptando o rechazando la notificación fuera del plazo máximo establecido.
9. El caso fortuito o de fuerza mayor debe ser invocada con posterioridad a la suscripción del contrato y durante la vigencia del contrato, siempre y cuando el hecho haya ocurrido dentro del plazo de ejecución contractual.

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

Cuando una situación de fuerza mayor o caso fortuito ha existido durante un período de más de seis (6) meses, podrá ser causal de rescisión o terminación anticipada del contrato.

Solicitud de suspensión de la ejecución del contrato

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

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

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

Convenios Modificatorios

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

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

2. Tratándose de contratos abiertos, las modificaciones a ser introducidas se regirán atendiendo a la reglamentación vigente.

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

Si no fuere posible acordar los términos del convenio modificatorio, la contratante podrá ejercer sus derechos establecidos

en el artículo 65 de la Ley N° 7021 de Suministro y de Contrataciones Públicas.

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

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. Si el proveedor no cumple con las obligaciones laborales, de seguridad social y/o de salud y seguridad ocupacional.
vii. 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 articulo 72 y concordantes de la Ley N° 7021/22.

Otras causales de terminación del contrato

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

No Aplica

Medio alternativo de Resolución de Conflictos a través del Avenimiento.

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

Medio Alternativo de Resolución de Conflictos a través de la Mediación

Las controversias, diferencias o reclamos que se susciten entre las partes con motivo del presente contrato, su interpretación, ejecución, cumplimiento, resolución o terminación, y que sean susceptibles de transacción, conciliación o mediación, podrán ser sometidas de manera voluntaria a un procedimiento de mediación, conforme a lo dispuesto en la Ley N° 1879/2002 “De Mediación”, en la Ley N° 7021/2022 “De Suministro y Contrataciones Públicas”, y a las condiciones establecidas en el presente contrato.

El procedimiento de Mediación se podrá llevar a cabo ante:

No Aplica

El mediador deberá pertenecer a las Listas del Poder Judicial o del CAMP, según la selección de sede establecida y actuará como tercero neutral e imparcial, de conformidad con la normativa aplicable.

El procedimiento de mediación se iniciará mediante solicitud de cualquiera de las partes y se sustanciará conforme al reglamento vigente de la sede seleccionada, el cual las partes declaran conocer y aceptar, incluyendo las disposiciones relativas a honorarios, gastos y costas, que se considerarán parte integrante de esta cláusula.

La mediación deberá concluir en un plazo máximo de treinta (30) días hábiles, contados a partir de la primera audiencia de mediación, plazo que podrá ser prorrogado por única vez, hasta por un período adicional de quince (15) días, únicamente mediante acuerdo expreso y escrito de las partes.

La mediación concluirá con la suscripción del acta de acuerdo, con la constancia de imposibilidad de acuerdo, o con la certificación

correspondiente emitida por la sede de mediación. Vencido el plazo máximo sin haberse alcanzado un acuerdo, o concluido el procedimiento sin solución de consensuada, las partes quedarán habilitadas para recurrir a las instancias correspondientes. Para la homologación y ejecución del acta de mediación, así como para el conocimiento de las controversias no resueltas mediante este mecanismo, las partes se someten a la jurisdicción de los tribunales competentes 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

El o los árbitros designados deberán pertenecer a la lista del cuerpo arbitral del CAMP, que decidirá conforme a derecho, siendo el laudo definitivo y vinculante para las partes.

Todas las controversias que deriven del presente contrato o que guarden relación con éste serán resueltas definitivamente por arbitraje, conforme con las disposiciones de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas", de la Ley N° 7.561 “De Arbitraje” y las condiciones del Contrato. Se aplicará el reglamento respectivo y demás disposiciones que regule dicho procedimiento al momento de ser requerido, declarando las partes conocer y aceptar los vigentes, incluso en orden a su régimen de gastos y costas, considerándolos parte integrante del presente contrato. Para la ejecución del laudo arbitral, o para dirimir cuestiones que no sean arbitrables, las partes se someterán a la jurisdicción de los tribunales de la ciudad de Asunción, República del Paraguay".

MODELO DE CONTRATO

Este modelo de contrato, constituye la proforma del contrato a ser utilizada de manera obligatoria, una vez adjudicado al proveedor y en los plazos dispuestos para el efecto por la normativa vigente, teniendo en cuenta que en los procedimientos de contratación cuyo objeto sea obras, locaciones o consultorías, deberán ser instrumentados mediante contratos y necesariamente deberán contar con una orden de inicio.

Así también, cuando en el procedimiento sea de menor cuantía y se deban emitir más de una orden de ejecución, independientemente al sistema de adjudicación, se deberá formalizar a través de un contrato, salvo aquellos casos previstos en el artículo 37 Inc. e) de la Ley N° 7021/22 ‘’De Suministro y Contrataciones Públicas’’

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.