

PLIEGO DE BASES Y CONDICIONES

Convocante:

Ministerio de Trabajo, Empleo y Seguridad Social (MTESS)
Ministerio de Trabajo Empleo y Seguridad Social

Nombre de la Licitación:

**LPN 09/2026 ADQUISICIÓN Y MONTAJE PARA LA
MODERNIZACIÓN INTEGRAL DE LA
INFRAESTRUCTURA DE RED DEL MTESS**
(versión 1)

ID de Licitación:

486592



Modalidad:

Licitación Pública Nacional

Publicado el:

26/09/2026

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

Versión 4

RESUMEN DEL LLAMADO

Datos de la Convocatoria

ID de Licitación:	486592	Nombre de la Licitación:	LPN 09/2026 Adquisición y Montaje para la Modernización Integral de la Infraestructura de Red del MTESS
Convocante:	Ministerio de Trabajo, Empleo y Seguridad Social (MTESS)	Categoría:	81000000 - Tecnologías de Información, Telecomunicaciones y Radiodifusiones
Unidad de Contratación:	Ministerio de Trabajo Empleo y Seguridad Social	Tipo de Procedimiento:	LPN - Licitación Pública Nacional

Etapas y Plazos

Lugar para Realizar Consultas:	A través del modulo correspondiente del SICP del Portal de Contrataciones Publicas (DNCP)	Fecha Límite de Consultas:	13/10/2026 12:00
Lugar de Entrega de Ofertas:	Luis Alberto de Herrera esq. Paraguari - Sede Central del MTESS - 3er. Piso UOC	Fecha de Entrega de Ofertas:	19/10/2026 07:30
Lugar de Apertura de Ofertas:	Luis Alberto de Herrera esq. Paraguari - Sede Central del MTESS - 3er. Piso UOC	Fecha de Apertura de Ofertas:	19/10/2026 08:00

Adjudicación y Contrato

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

Datos del Contacto

Nombre:	Unidad Operativa de Contrataciones	Cargo:	MTESS
Teléfono:	7290100	Correo Electrónico:	uoc@mtess.gov.py

DATOS DE LA CONVOCATORIA

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

Datos de la Convocatoria

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

Difusión de los documentos de la Convocatoria

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

Contratación Pública 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:

Se permitirán catálogos, anexos técnicos o folletos en idioma diferente al castellano y su traducción.

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 registrará 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 registrará 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 inscritos 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:

Fecha o período de realización: 08 de octubre de 2026

Lugar: Sede de la MTESS - Luis A. de Herrera e/ Paraguarí

Hora: 09:00 horas. No sera reiniciada.

Procedimiento: El relevamiento del edificio de cinco niveles, canalizaciones, racks, puntos de energía, equipos existentes, restricciones de acceso y condiciones de coexistencia con videovigilancia y control de acceso para que el oferente dimensiona correctamente materiales, actividades, recursos y riesgos de la implementación llave en mano, evitando omisiones que luego afecten el plazo o el costo de ejecución

Nombre y contacto del funcionario responsable de guiar la visita: Juan Gabriel Arellano Zelaya - CARGO: Jefe de Tecnología de la Información y Comunicación

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:

Se solicita Autorización del Fabricante de las marcas **de los equipos de networking y solución de cableado** ofertadas, dirigida a la Institución con referencia al proceso para todos los ítems y/o subítems

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:

Como minimo 36 (treinta y seis) meses.-

Plazo de reposición de bienes

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

5 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:

Garantía directa del fabricante por treinta y seis (36) meses.

Cobertura de Seguro de los bienes

La cobertura de seguro requerida a los bienes será:

No Aplica

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

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, inscritos 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 N° 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 N° 7021/22, el comité de evaluación realizará el siguiente análisis:

1° 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.

2° 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 incurso en las causales previstas en los Arts. 17 y 21 de la Ley N° 7021/22.

3° Verificará por los medios disponibles, si el oferente y los demás sujetos individualizados en las prohibiciones o limitaciones contenidas en los incisos 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.

4° Si se constatará 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.

5° 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.

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

7° 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 N° 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 N° 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:

Bien/Servicio ofertado.	Costo expresado en la moneda de la oferta.
Elementos de Valor Fijo	
Mano de obra	
Inmuebles	
Maquinarias	
Herramientas	
Vehículos	
Equipos informáticos	
Muebles	
Seguros	
Servicios básicos	
Elementos de Valor Variable	
Insumos	
Mantenimiento	

Gastos administrativos	
Gastos de venta	
Total de costos	
Utilidad esperada	
Precio del bien/servicio antes de impuestos	
Impuestos	
Precio final del bien/servicio impuestos incluidos	

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

A) Contribuyente de IRACIS/IRE RG por los años que corresponda deberán cumplir con el siguiente parámetro:

a. Ratio de Liquidez: activo corriente / pasivo corriente. Deberá ser igual o mayor que 1, en promedio, en los últimos años (2023, 2024 y 2025)

b. Endeudamiento: pasivo total / activo total. No deberá ser mayor a 0,80 en promedio, en los últimos años (2023, 2024 y 2025)

c. Rentabilidad: Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital. El promedio en los últimos años (2023, 2024 y 2025) no deberá ser negativo.

B) Contribuyentes de IRPC / IRE SIMPLE por los años que corresponda deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

-Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales requeridos (2023, 2024 y 2025).

C) Contribuyentes de IRP/IRP RSP por los años que corresponda deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales requeridos (2023, 2024 y 2025).

D) Contribuyentes de exclusivamente IVA General deberá cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales (2023, 2024 y 2025).

EN CASO DE CONSORCIOS; todos los integrantes que lo componen deberán cumplir con los requisitos financieros indicados

Requisitos documentales para la evaluación de la capacidad financiera

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

a

Certificado de Cumplimiento Tributario vigente a la fecha y hora tope de presentación de ofertas

b

Para todos los casos, presentar en carácter de declaración jurada, un cuadro descriptivo de los índices requeridos según corresponda, incluyendo los valores aplicados para la obtención del/de los promedios o índice del/de los ratios requeridos, elaborado y firmado por un profesional de las áreas de ciencias económicas, administrativos, contables o afines. Además deberá agregar copia de las documentaciones solicitadas para cada caso como ser balances contables y/o formularios de declaración, aplicado al calculo efectuado, las cuales deberán ser legibles, como ser:

Balance General y Cuadro de Estado de Resultados de los años 2023, 2024 y 2025 para contribuyente de IRACIS /IRE RG

Formulario 501 (2023, 2024 y 2025) IRE Simple.

Formulario 515 (2023, 2024 y 2025) IRP RSP.

Para contribuyentes de IVA general: IVA General de los últimos 3 años (2023, 2024 y 2025)

Constancia de una entidad bancaria de plaza, financiera o cooperativa en la que confirme que posee una línea de crédito aprobada, por un valor igual o superior al 30% del valor total de la oferta.

Experiencia requerida

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

Demostrar experiencia en la ejecución o implementación de proyectos de naturaleza y complejidad técnica similar al objeto del llamado, que incluyan, según corresponda, actividades de suministro, instalación, configuración y/o soporte de infraestructura de red y/o seguridad, ejecutados para entidades públicas o privadas acompañado con su acta de recepción final y/o constancia. La experiencia acumulada deberá representar, como mínimo, el 40% del monto total ofertado en la presente licitación y podrá corresponder a trabajos ejecutados durante los años 2023, 2024 y 2025. No es necesario contar en los 3 años, con un solo contrato se cumple con el requisito.

En el caso de los OFERENTES EN CONSORCIO la empresa Líder deberá cumplir con el 80% de los requisitos de calificación en cuanto a la Experiencia solicitada por la convocante, mientras que los demás miembros del consorcio deberán cumplir con el 20% de lo solicitado (requerimientos mínimos).

Requisitos documentales para la evaluación de la experiencia

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

1. Copias de contratos, facturas y/o recepciones finales que acrediten la ejecución o implementación satisfactoria de proyectos de naturaleza y complejidad técnica similar al objeto del llamado, incluyendo, según corresponda, actividades de suministro, instalación, puesta en funcionamiento y/o soporte de infraestructura de red y/o seguridad, para entidades públicas o privadas. La documentación presentada deberá permitir verificar una experiencia acumulada equivalente, como mínimo, al 40% del monto total ofertado, correspondiente a trabajos ejecutados durante los años 2023, 2024 y 2025. En caso de contrato privado, se deberá incluir facturas del contrato.

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:

1. Planilla de Datos Garantizados, debidamente completadas y firmadas conforme al formato establecido en la Sección de Suministros requeridos Especificaciones Técnicas (considerado como documento sustancial, para la evaluación técnica).
2. Certificado Laboral vigente
3. Certificación en Gestión de Calidad
4. Certificación en Gestión de Seguridad de la información.
5. El oferente deberá presentar la carta de Autorización de los equipos de networking y solución de cableado, dirigida a la Institución y con referencia al proceso.
6. El oferente deberá contar con los siguientes profesionales certificados, los mismos deberán formar parte del plantel de la empresa con una antigüedad de al menos 1 (un) año, demostrable mediante planilla de IPS. No se aceptarán profesionales subcontratados.:
 - a. Arquitecto o especialista senior en redes, 1 (uno): Nivel profesional o superior en conmutación y enrutamiento empresarial: CCNP Enterprise, HPE Aruba Networking Certified Switching Professional, Fortinet FCP/FCSS Network Security, Juniper JNCIP-ENT, Extreme ECS, o certificación equivalente del fabricante ofertado.
 - b. Técnicos en cableado estructurado, 2 (dos): Certificación vigente de instalador emitida por BICSI (ITS Installer 2 o superior) o por el fabricante del sistema de cableado ofertado, o acreditación de tres (3) años de experiencia en instalación y certificación de enlaces Categoría 6A.
 - c. Especialista en seguridad de red, 2 (dos): CompTIA Security+ y/o Cisco CyberOps Associate o Professional y/o Fortinet FCP Network Security y/o GIAC GSEC, o certificación de nivel profesional del fabricante de la solución ofertada. Deberá contar con al menos 1 (un) técnico certificado en CompTIA A+ o superior.
 - d. Especialista en la solución de seguridad perimetral ofertada, 1 (uno): Certificación de nivel profesional del fabricante ofertado que acredite la capacidad para implementar la solución.
 - e. Responsable de proyecto, 1 (uno): PMP, PRINCE2 Practitioner, IPMA nivel C o superior, PMI-ACP, o acreditación

de conducción de al menos dos (2) proyectos de infraestructura tecnológica de alcance comparable en los últimos cinco años.

Obs. Las certificaciones deben poder ser verificadas, no se aceptará certificaciones sin medios de validación.

Requisitos documentales para evaluar el criterio de capacidad técnica

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

1. Planilla de Especificaciones Técnicas debidamente completada y firmada conforme al formato establecido en la Sección de Suministros Requeridos - Especificaciones Técnicas.
2. El Oferente deberá presentar el Certificado Laboral vigente, expedido conforme a lo establecido en la Resolución MTESS N.º 781/2025.
3. El oferente deberá presentar una certificación vigente de un sistema de gestión que garantice la calidad en la prestación de servicios, emitida por una entidad certificadora competente, acreditada y verificable se debe evidenciar criterios orientados a asegurar la calidad de la gestión de procedimientos de Provisión e integración de bienes y/o servicios, abarcando mínimamente la integración de 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 prácticas reconocidas para la gestión de la calidad en la Provisión e integración de bienes y/o servicios
4. 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 se debe evidenciar criterios orientados a asegurar la confidencialidad, integridad y protección de los datos, abarcando mínimamente la integración de 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 prácticas reconocidas para la gestión de la seguridad, confidencialidad e integridad de la información y de los datos tratados.
5. Autorización del Fabricante de los equipos de networking y solución de cableado, dirigida a la Institución y con referencia al proceso.
6. Planilla del Instituto de Previsión Social correspondiente al mes anterior vencido a la fecha de la apertura de ofertas en donde figure el técnico propuesto, acompañado de la siguiente documentación: - Copia del certificado. - Currículum Vitae del técnico propuesto acompañado de todos los documentos respaldatorios que avalen su formación profesional. - Copia de cédula de identidad del técnico.

Otros criterios que la convocante requiera

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

No Aplica

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:

- Identificar el nombre, cargo y la dependencia de la Institución de quien solicita el procedimiento de contratación a ser publicado. Denis Omar Gonzalez Gonzalez, Director, Direccion de Tecnologia de la Información y Comunicación
- Justificación de la necesidad que se pretende satisfacer mediante la contratación a ser realizada: se ha determinado la necesidad de realizar una renovación integral de la infraestructura física y lógica de red de la sede institucional, principalmente debido a la antigüedad de la infraestructura actualmente instalada, la obsolescencia tecnológica de varios de sus componentes, las fallas recurrentes y las deficiencias técnicas acumuladas a lo largo del tiempo. Estas condiciones se traducen actualmente en interrupciones e inestabilidad de los servicios de conectividad, degradación del rendimiento de la red, limitaciones de capacidad, dificultades para la administración y monitoreo, así como mayores riesgos de indisponibilidad de los servicios tecnológicos institucionales. Asimismo, la permanencia de tecnologías y componentes antiguos limita la posibilidad de incorporar nuevas funcionalidades, incrementar las velocidades de transmisión, fortalecer los mecanismos de seguridad y acompañar adecuadamente el crecimiento de las necesidades tecnológicas del MTESS
- Justificación de la planificación: (si se trata de un procedimiento de contratación periódico o sucesivo, o si el mismo responde a una necesidad temporal). Necesidad Temporal.
- Las especificaciones técnicas deberán estar sustentadas en el dictamen técnico, requerido al momento de la comunicación de la convocatoria.

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:

Objetivo del Proyecto

El presente proyecto tiene por objeto la modernización integral de la infraestructura de red del Ministerio de Trabajo, Empleo y Seguridad Social (MTESS), mediante la provisión, instalación, configuración, integración y puesta en funcionamiento de una solución tecnológica moderna, segura, estable, redundante y escalable, capaz de responder a las necesidades actuales y futuras de la institución.

La ejecución del proyecto se fundamenta en la necesidad de sustituir la infraestructura existente, debido a las fallas recurrentes y deficiencias técnicas constatadas tanto en el cableado estructurado como en los equipos de red. Estas condiciones ocasionan interrupciones, inestabilidad y degradación del rendimiento de los servicios de conectividad, además de dificultar la administración y limitar la capacidad de crecimiento de la red institucional.

Por otra parte, la conectividad inalámbrica existente ha resultado insuficiente para atender adecuadamente el incremento de funcionarios, usuarios y dispositivos conectados de manera simultánea, lo que genera limitaciones de cobertura, capacidad y estabilidad. En consecuencia, se requiere fortalecer la red inalámbrica mediante equipos de mayor capacidad, con administración y monitoreo centralizados.

Los trabajos serán ejecutados en la sede del MTESS, ubicada sobre la calle Luis A. de Herrera e/ Paraguari, en un edificio compuesto por cinco pisos, donde se realizarán todas las actividades de provisión, instalación, adecuación, configuración y puesta en funcionamiento previstas en el presente proyecto.

El alcance no se limita al reemplazo del cableado existente, sino que comprende la renovación integral de la infraestructura física de comunicaciones en los cinco pisos del edificio, la incorporación de equipos de red y protección configurados en alta disponibilidad (HA), el fortalecimiento de la conectividad inalámbrica y la implementación de plataformas destinadas a proteger los accesos, los equipos, los sistemas y la información institucional.

Con esta modernización se busca mejorar el rendimiento, la disponibilidad y la capacidad de administración de la red, reducir los riesgos de interrupción y disponer de una infraestructura preparada para acompañar el crecimiento y la incorporación de nuevos servicios tecnológicos.

Alcance del Proyecto

1. Modernización del cableado estructurado

La modernización del cableado estructurado deberá comprender la instalación, terminación, identificación y certificación de 300 puntos dobles de red, distribuidos desde la planta baja hasta el cuarto piso.

El cableado existente deberá ser desinstalado y reemplazado por una nueva infraestructura de cableado blindado de Categoría 6A, diseñada para soportar velocidades de transmisión de hasta 10 Gbps mediante tecnología Ethernet.

Cada enlace deberá ser identificado y certificado individualmente mediante equipos especializados, con el propósito de verificar su correcto funcionamiento y acreditar el cumplimiento de los parámetros técnicos y niveles de rendimiento establecidos, como mínimo, en las normas ANSI/TIA-942, ANSI/TIA/EIA-568-C, ANSI/TIA/EIA-569-B y ANSI/TIA-606-B.

Asimismo, se deberá contemplar la sustitución de los racks seccionales existentes por racks nuevos, debidamente dimensionados para alojar, organizar y proteger los equipos y componentes que conformarán la nueva infraestructura de red.

El alcance deberá incluir la migración integral de los equipos y servicios actualmente en funcionamiento, incluyendo las cámaras de videovigilancia y los equipos de control de acceso, hacia la nueva infraestructura de red.

2. Mayor velocidad y capacidad de transmisión

La interconexión de los switches ubicados en los diferentes pisos deberá realizarse mediante enlaces de fibra óptica,

debidamente instalados, terminados, identificados y certificados. Estos enlaces conformarán la columna vertebral o backbone de la red institucional, garantizando una comunicación de alta velocidad, estable y confiable entre los distintos niveles del edificio.

Esta infraestructura deberá permitir transmitir grandes volúmenes de información con mayor velocidad, estabilidad y disponibilidad, reduciendo posibles congestiones entre pisos y dejando la red preparada para futuras ampliaciones y la incorporación de nuevos servicios tecnológicos.

3. Continuidad de los servicios institucionales

Se deberán instalar dos switches de Core en el Data Center del MTESS, configurados en alta disponibilidad, los cuales constituirán el núcleo principal de la red institucional. Esta configuración redundante deberá garantizar que, ante la falla de uno de los equipos, el segundo mantenga la continuidad operativa de la red, reduciendo el riesgo de interrupciones generales.

Asimismo, se incorporarán 10 switches de acceso de 48 puertos con capacidad PoE, destinados a proporcionar conectividad a los puestos de trabajo, puntos de acceso inalámbrico y demás dispositivos de red.

4. Mejoramiento de la conectividad inalámbrica

El mejoramiento de la conectividad inalámbrica deberá contemplar la instalación de 40 puntos de acceso Wi-Fi, con administración, configuración y monitoreo centralizados.

Estos equipos permitirán mejorar la cobertura, capacidad, estabilidad y seguridad de la red inalámbrica, proporcionando conectividad eficiente a los funcionarios y dispositivos debidamente autorizados dentro de las instalaciones del MTESS.

5. Modernización de la central telefónica IP

Se deberá implementar una central telefónica IP basada en protocolo SIP a fin de reutilizar los terminales telefónicos existentes, destinada a centralizar y optimizar las comunicaciones de voz de la institución. La solución permitirá administrar extensiones, usuarios, llamadas y servicios telefónicos desde una plataforma centralizada, facilitando su gestión, monitoreo y mantenimiento.

La central deberá integrarse con la nueva infraestructura de red del MTESS y suministrarse con todas las licencias, módulos, componentes y accesorios necesarios para su correcto funcionamiento. Asimismo, deberá garantizar la calidad de las comunicaciones, la interoperabilidad con los dispositivos existentes o proyectados y la posibilidad de ampliación conforme al crecimiento futuro de la institución.

Esta implementación permitirá modernizar el sistema de telefonía institucional, mejorar la disponibilidad del servicio, reducir los costos operativos y facilitar la incorporación de nuevas extensiones y funcionalidades de comunicación.

Esta protección permitirá reducir el riesgo de apagados inesperados, daños en los equipos y pérdidas temporales de conectividad.

6. Fortalecimiento de la seguridad perimetral

Se deberán incorporar dos firewalls configurados en alta disponibilidad, destinados a proteger la comunicación entre la red institucional, Internet y otros entornos externos.

Los equipos deberán permitir la inspección y el control del tráfico, la administración de aplicaciones y accesos, la prevención de intrusiones, el bloqueo de amenazas y el establecimiento de conexiones remotas seguras. La configuración redundante permitirá mantener la protección y la continuidad del servicio ante la falla de uno de los equipos.

7. Solución integral de gestión, monitoreo y protección tecnológica

Se deberá proveer una plataforma integral que permita administrar y controlar las cuentas con privilegios elevados; proteger las credenciales administrativas; registrar y auditar sesiones; y otorgar accesos temporales de acuerdo con los permisos establecidos.

La solución deberá centralizar, correlacionar y analizar los registros generados por los equipos, sistemas y aplicaciones institucionales, permitiendo identificar actividades anómalas, generar alertas y facilitar la investigación de incidentes y los procesos de auditoría.

Asimismo, deberá controlar la transferencia de información institucional en un mínimo de **500 estaciones de trabajo**,

mediante dispositivos USB, correo electrónico, servicios en la nube, impresoras, Bluetooth y otros canales, con el propósito de prevenir su pérdida, extracción, utilización indebida o divulgación no autorizada.

La plataforma deberá incorporar capacidades de detección, investigación y respuesta centralizada para **500 usuarios**, ante programas maliciosos, intentos de explotación y comportamientos sospechosos, facilitando la aplicación oportuna de medidas de contención.

LISTA DE BIENES

Descripción del Bien	Unid. De Medida	Cantidad
Modernización Integral de la Infraestructura de Red del MTESS bajo la Modalidad Llave en Mano	Unidad de Medida Global	1

El Oferente deberá proveer, instalar, configurar, integrar y poner en funcionamiento todos los equipos y componentes contemplados en el proyecto.

Asimismo, deberá proporcionar soporte técnico especializado, capacitación a los funcionarios designados por la Convocante y la documentación técnica correspondiente, incluyendo planos, diagramas, inventarios, configuraciones, respaldos e informes de certificación.

A continuación, se detalla los materiales y servicios mínimos requeridos que debe ser considerada para la elaboración de la oferta:

Descripción del Bien	Unid. De Medida	Cantidad
Switch Core en HA	Unidad	2
Switch 48P PoE	Unidad	10
Firewall en HA	Unidad	2
APs Wifi	Unidad	40
Central Telefónica IP	Unidad de Medida Global	1
Cableado Estructurado	Unidad de Medida Global	1
Desinstalación de Cableado Existente para su sustitución	Unidad de Medida Global	1

Solución Integral de Protección y Control.	Unidad de Medida Global	1
--	-------------------------	---

Los productos a ser requeridos cuentan con las siguientes especificaciones técnicas:

Switch Core en HA

Perfil de uso MITIC seleccionado: SW-005-01 Switch LAN Ethernet orientado a redes LAN de gran escala / Orientado a Switch de Core.

ITEM	ESPECIFICACIONES TÉCNICAS	CARACTERÍSTICAS	MÍNIMO EXIGIDO
1	Marca	Especificar	Exigido
2	Modelo	Especificar	Exigido
3	Número de Parte del Fabricante del / Equipo	No se requiere	No se requiere
4	Origen / Procedencia	Especificar	Exigido
5	Cantidad	2 (dos) unidades	Exigido
6	Cantidad de Puertos Tipo 1 / Velocidad Tipo 1 / Conector/Medio Tipo 1	4 puertos; velocidades 40G/100G; conectores Base-X mediante QSFP+/QSFP28.	Exigido
7	Cantidad de Puertos Tipo 2 / Velocidad Tipo 2 / Conector/Medio Tipo 2	24 puertos; velocidades 1G/10G; conectores Base-X mediante SFP/SFP+.	Exigido
9	Transceivers Enchufables	Incluir 16 (dieciséis) transceivers 10GE SFP+, dúplex monomodo, alcance mínimo 10 km, además de los accesorios necesarios para la puesta en servicio.	Exigido

10	Capacidad de Conmutación	Capacidad de switching mínima de 1,7 Tbps; throughput mínimo de 1,3 Mpps; arquitectura no bloqueante. Memoria mínima: 16 GB RAM, 32 GB Flash/Storage y packet buffer de 32 MB.	Exigido
12	Control de Flujo en Capa 2	Control de flujo para prevenir acumulación excesiva de congestión y evitar el almacenamiento prolongado de paquetes en buffer.	Exigido
13	Apilado (Stacking)	No se requiere	No se requiere
14	Cantidad de MAC Addresses:	147.000 direcciones MAC como mínimo.	Exigido
15	VLANs	4.000 VLAN ID como mínimo; IEEE 802.1v; MVRP; Private VLAN (PVLAN) y QinQ.	Exigido
16	Lazos en Capa 2	IEEE 802.1D; IEEE 802.1w; IEEE 802.1s; Rapid Per-VLAN Spanning Tree (RPVST+) y ERPS.	Exigido
17	Tramas Ethernet	Jumbo Frames de 9K bytes.	Exigido
18	Agregación de Enlaces (LAG)	IEEE 802.3ad LACP; soporte de al menos 52 grupos, hasta 8 enlaces por grupo, selección de algoritmo de hashing L1-L4 y agregación multichasis para el clúster.	Exigido
19	Detección de Dispositivos	LLDP.	Exigido
20	Ruteo IP	24.500 rutas IPv4 y 12.250 rutas IPv6 como mínimo; rutas estáticas IPv4/IPv6; ECMP; OSPF/OSPFv2/OSPFv3; BGP-4/MP-BGP; RIPv2/RIPng; Policy-Based Routing; Dual Stack IPv4/IPv6 y soporte de NLB.	Exigido
21	Tráfico y Ruteo IP	IGMP v1/v2/v3; IGMP Snooping; PIM SM, SSM y DM para IPv4/IPv6; MLD v1/v2 y MSDP.	Exigido
22	Detección de Fallos	BFD (Bidirectional Forward Detection).	Exigido
23	Resolución de Direcciones Capas 2 y 3	ARP estático, Gratuitous ARP y Proxy ARP.	Exigido
24	VPN	GRE (Generic Routing Encapsulation).	Exigido

25	Controller Wireless LAN (WLAN)	No se requiere	No se requiere
26	Calidad de Servicio (QoS)	Strict Priority; DWRR; DCB/DCBX; PFC; ETS; IEEE 802.1p; DSCP; CoS; IP SLA; soporte para iSCSI/Lossless iSCSI, RoCE v1/v2 y NVMe over Fabrics.	Exigido
27	Listas de Acceso	Listas de Control de Acceso (ACL) para IPv4 e IPv6, incluyendo protección del plano de control para SSH, SNMP, NTP y servidor web.	Exigido
28	Monitoreo	sFlow (RFC 3176), IPFIX y motor local de monitoreo y análisis de eventos que puedan afectar la salud de la red.	Exigido
29	Monitoreo de Tráfico Espejado	Port mirroring de tráfico entrante y saliente hacia puertos de monitoreo locales o remotos; soporte de hasta 4 grupos de mirror.	Exigido
31	Autenticación	RADIUS, TACACS+ y RadSec para administración; control de acceso por puerto y mecanismos de autenticación compatibles.	Exigido
32	Seguridad	Gestión segura mediante SSHv2, HTTPS y SNMPv3; TPM; EST; Port Security; MAC Lockdown; BPDU Filter/Guard; DHCP Snooping; Loop Protection; FIPS 140-2 y control de tormentas unicast/broadcast/multicast.	Exigido
33	Administración	Administración mediante CLI, GUI y nube; puerto serial RJ45, consola USB-C, puerto Ethernet RJ45 para administración fuera de banda y puerto USB para archivos. API REST, aprovisionamiento de día cero, niveles de privilegio, Syslog, SNMP v2c/v3, TFTP, SFTP y SSH.	Exigido
34	NTP	NTP.	Exigido
35	DHCP	DHCP Relay, DHCP Server y DHCP Client.	Exigido
36	DNS	Cliente y servidor DNS.	Exigido
37	Automatización	Interfaz API REST integrada y programable; aprovisionamiento de día cero y automatización de tareas de configuración/gestión mediante mecanismos equivalentes.	Exigido
38	Otras Características de Automatización	No se requiere	No se requiere
39	Virtualización	VXLAN estático y dinámico con BGP-EVPN.	Exigido

40	Eficiencia Energética	No se requiere	No se requiere
41	Condiciones de Operación	Temperatura de operación de 0 °C a 40 °C; humedad de operación de 15% a 95% sin condensación.	Exigido
42	Mantenimiento	No se requiere	No se requiere
43	Alimentación Eléctrica	Alimentación AC 100-127 VAC y 200-240 VAC, 50/60 Hz.	Exigido
44	Redundancias	Dos fuentes de alimentación reemplazables en caliente; tres arreglos de ventiladores reemplazables en caliente; arquitectura distribuida y redundante con dos switches sincronizados, actualizaciones en operación, UDLD, BFD, VRRP, soporte NLB y doble imagen de sistema operativo.	Exigido
45	Software	El sistema operativo deberá incluir el licenciamiento de todos los puertos y características de servicio exigidas. Los servicios que requieran licenciamiento avanzado deberán indicarse expresamente.	Exigido
46	Certificaciones	RoHS. El fabricante de los equipos de comunicación deberá figurar en el informe de Cuadrante Mágico de Gartner (Wired and Wireless LAN Access Infrastructure) en cualquiera de sus cuadrantes o en un informe de analista de mercado de reconocido prestigio internacional equivalente, dentro de los últimos dos años. El oferente deberá acreditar mediante hojas de datos oficiales el cumplimiento de las especificaciones operativas y la interoperabilidad bajo estándares abiertos (IEEE, IETF). Se deberá presentar Autorización del Fabricante dirigida al MTESS y con referencia al presente llamado.	Exigido
47	Chasis	Formato rackeable máximo 1U e inclusión de todos los accesorios para montaje y operación en rack estándar de 19".	Exigido
48	Montaje e Instalación	El proveedor deberá incluir todos los componentes, licencias, configuraciones y servicios necesarios para garantizar la alta disponibilidad de la solución ofertada.	Exigido
49	Documentación	Documentación técnica oficial del fabricante suficiente para verificar las características ofertadas, el cumplimiento de estándares abiertos y las condiciones de licenciamiento.	Exigido
50	Garantía de fábrica	Garantía directa del fabricante por treinta y seis (36) meses.	Exigido

51	Ciclo de Vida	No se requiere	No se requiere
----	---------------	----------------	----------------

Switches 48P PoE

Perfil de uso MITIC seleccionado: SW-004-01 Switch LAN Ethernet orientado a redes LAN de oficinas pequeñas y medianas / Switch de Acceso y Agregación.

ITEM	ESPECIFICACIONES TÉCNICAS	CARACTERÍSTICAS	MÍNIMO EXIGIDO
1	Marca	Especificar	Exigido
2	Modelo	Especificar	Exigido
3	Número de Parte del Fabricante del / Equipo	No se requiere	No se requiere
4	Origen / Procedencia	Especificar	Exigido
5	Cantidad	10 (diez) unidades	Exigido
6	Cantidad de Puertos Tipo 1 / Velocidad Tipo 1 / Conector/Medio Tipo 1	4 puertos SFP+ 1G/10G, conectores Base-X.	Exigido
7	Cantidad de Puertos Tipo 2 / Velocidad Tipo 2 / Conector/Medio Tipo 2	48 puertos RJ45: 32 puertos 10/100/1000Base-T y 16 puertos 100/1000/2500Base-T.	Exigido
8	Transceivers Enchufables	No se requiere	No se requiere
9	Capacidad de Conmutación	Capacidad de conmutación igual o superior a 220 Gbps.	Exigido
10	Puertos RJ45	No se requiere	No se requiere
11	Control de Flujo en Capa 2	IEEE 802.3x Flow Control.	Exigido
12	Cantidad de MAC Addresses	30.000 direcciones MAC en hardware como mínimo.	Exigido

13	Apilado (Stacking)	No se requiere	No se requiere
14	VLANs	256 VLAN simultáneas como mínimo; rango de VLAN ID 1-4000; IEEE 802.1Q VLAN Tagging.	Exigido
15	Lazos en Capa 2	IEEE 802.1D MAC Bridging/STP e IEEE 802.1w RSTP.	Exigido
16	Otros Lazos en Capa 2	IEEE 802.1s MSTP.	Exigido
17	Tramas Ethernet	Jumbo Frames de 9K bytes.	Exigido
18	Agregación de Enlaces (LAG)	IEEE 802.3ad Link Aggregation con LACP; cantidad mínima de 8 puertos pertenecientes a grupos LAG.	Exigido
19	Detección de Dispositivos	No se requiere	No se requiere
20	Ruteo IP	Soporte de rutas estáticas.	Exigido
21	Tráfico y Ruteo IP	IGMP Snooping.	Exigido
22	Resolución de Direcciones Capas 2 y 3	No se requiere	No se requiere
23	VPN	No se requiere	No se requiere
24	Calidad de Servicio (QoS)	No se requiere	No se requiere
25	Listas de Acceso	No se requiere	No se requiere
26	Monitoreo	RFC 1643 Ethernet-like Interface MIB; RFC 1213 MIB-II; RFC 1493 Bridge MIB; RFC 2618 RADIUS Authentication Client MIB; SNMP v1/v2c.	Exigido
27	Monitoreo de Tráfico Espejado	No se requiere	No se requiere

28	Autenticación	RFC 2865 RADIUS y autenticación IEEE 802.1X.	Exigido
29	Seguridad	No se requiere	No se requiere
30	Administración	Registro de dispositivos en plataforma de gestión centralizada; visibilidad del estado en línea; RFC 854 Telnet cliente/servidor; SNMP v1/v2c y MIBs indicadas.	Exigido
31	NTP	No se requiere	No se requiere
32	DHCP	DHCP Client y DHCP Relay.	Exigido
33	Automatización	No se requiere	No se requiere
34	Virtualización	No se requiere	No se requiere
35	Eficiencia Energética	No se requiere	No se requiere
36	Condiciones de Operación	Temperatura de operación 0 a 45 °C (+/- 5%); humedad de operación 10% a 85% o superior.	Exigido
37	Mantenimiento	No se requiere	No se requiere
38	Alimentación Eléctrica	Soporte PoE/PoE+ bajo IEEE 802.3af/802.3at, con power budget mínimo disponible para consumo de puertos PoE+ de 740 W.	Exigido
39	Redundancias	No se requiere	No se requiere
40	Software	Administración y monitoreo mediante plataforma de gestión centralizada, con registro del equipo y visualización de su estado en línea.	Exigido
41	Certificaciones	FCC, CB, UL, RCM, ISED, KC, BSMI, VCCI, NOM y CE.	Exigido

42	Chasis	No se requiere	No se requiere
43	Montaje e Instalación	El oferente deberá entregar, instalar y configurar el equipo de acuerdo con las indicaciones y con el Plan de Trabajo aprobado.	Exigido
44	Documentación	No se requiere	No se requiere
45	Garantía de fábrica	Garantía directa del fabricante por treinta y seis (36) meses.	Exigido
46	Ciclo de Vida	No se requiere	No se requiere

Firewall en HA

Descripción	Descripción Técnica	Mínimo Exigido
Cantidad:	2 (dos) unidades	
Marca:	Especificar	
Modelo:	Especificar	
Procedencia:	Especificar	
Hardware	Procesamiento: el equipo deberá disponer de arquitectura de aceleración por hardware para procesamiento de tráfico y funciones de seguridad, mediante uno o más procesadores especializados o mecanismos técnicamente equivalentes.	Exigido
	RAM: 12 GB DDR4	Exigido
	Almacenamiento: tipo SSD integrados de al menos 120 GB	Exigido
	Puertos Ethernet:	Exigido
	8xGbE cobre +	

	Puertos de E/S:	Exigido
	1x COM RJ45	
	1 X RJ45 MGMT	
	2 x USB 3.0 (frente)	
	Fuente de alimentación: Auto-Ranging interno 110-240VAC, 50-60Hz. Hot Swap con posibilidad de alimentación redundante.	Exigido
	Certificaciones de producto: CB, CE, UKCA, UL, FCC, ISED, VCCI, KC, RCM, NOM, Anatel, CCC, BSMI, TEC, SDPPI	Exigido
	Firewall Throughput - 47.000 Mbps como mínimo.	Exigido
	IPS throughput- 10.500 Mbps como mínimo.	Exigido
	VPN throughput - 25.000 Mbps como mínimo.	Exigido
	Throughput contra amenazas 7.000 Mbps como mínimo.	Exigido
	Conexiones simultáneas 12.000.000 como mínimo.	Exigido
	Nuevas conexiones/seg - 180.000 como mínimo.	Exigido
	Máximo de usuarios con licencia: sin restricciones	Exigido
Administración General	Interfaz de usuario y gestión de reglas de Firewall optimizadas y diseñadas específicamente para grandes conjuntos de reglas agrupadas con indicadores de aplicación y características de las reglas de un vistazo	Exigido
	Autenticación de dos factores (contraseña de un solo uso - OTP) para acceso de administrador, portal de usuarios, IPSec y VPN SSL	Exigido
	Herramientas avanzadas de solución de problemas en GUI trouble-shooting (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
Soporte de HA en AWS mediante AWS Transit Gateway	Exigido
Soporte para enlaces redundantes en HA	Exigido
Búsqueda de objetos host y objetos de servicio	Exigido
Almacenamiento mejorado de archivos .log	Exigido
Compatibilidad mejorada con interfaces 40G	Exigido
Interfaz de línea de comandos (CLI) completa accesible desde la GUI	Exigido
Administración basada en roles (Role-based)	Exigido
Notificación automática de actualizaciones de firmware con un sencillo proceso de actualización automatizado y funciones de roll-back	Exigido
Auto-Rollback en actualizaciones de Firmware fallidas	Exigido
Definiciones de objetos de sistema reutilizables para redes, servicios, hosts, periodos de tiempo, usuarios y grupos, clientes y servidores.	Exigido
Portal de autoservicio (Self-service) para usuarios	Exigido
Seguimiento de cambios en la configuración	Exigido
Control flexible del acceso de los dispositivos a los servicios por zonas	Exigido
opciones de Notificaciones vía Email o Traps de SNMP	Exigido
soporte a SNMPv3 y Netflow	Exigido

Soporte de gestión central a través de la consola unificada basada en nube	Exigido
Notificaciones automáticas por correo electrónico de cualquier evento importante	Exigido
Configuraciones de Backup y restore:de manera local, via FTP o email; bajo demanda diaria semanal o mensual.	Exigido
Mejoras en los Backups y Restauraciones	Exigido
API para integraciones con terceros	Exigido
Renombre de Interfaces	Exigido
Opción de acceso remoto para el grupo de soporte del fabricante	Exigido
Gestión de licencias basada en nube a través del portal de licencias	Exigido
Soporte a Syslog	Exigido
Monitoreo en tiempo real de los flujos (Real-Time Flow)	Exigido
Indicadores de tráfico tipo semáforo	Exigido
Información instantánea de un solo vistazo	Exigido
Interacción rápida con cualquier widget del Centro de Control	Exigido
SNMP con una MIB personalizada y soporte para túneles VPN IPSec	Exigido
Soporte de nuevas instancias de AWS (C5/M5 y T3)	Exigido
Soporte para plantillas de formación en la nube	Exigido

Compatibilidad con zonas WAN virtuales en gateways personalizados para el uso de un solo brazo tras la instalación	Exigido
Compatibilidad con una amplia gama de plataformas de virtualización y también se puede instalar como dispositivo de software en su propio hardware Intel x86.	Exigido
Disponibilidad en el Marketplace de AWS con licenciamiento (PAYG) pago por uso o con la opción de (BYOL) traiga su propia licencia, para ajustarse según sus necesidades	Exigido
Certificado y optimizado para Azure y disponible en Microsoft Azure Marketplace. Puede realizar una prueba gratuita o utilizar las flexibles opciones de licencia PAYG o BYOL.	Exigido
Soporte a Nutanix AHV y Nutanix Flow	Exigido
Contraseña con algoritmo hash más robusto (<i>requiere un cambio de contraseña</i>)	Exigido
Las opciones de despliegue deberán incluir dispositivo físico, software o virtual y compatibilidad con entornos de nube pública, incluyendo Microsoft Azure o plataformas equivalentes.	Exigido
Habilitación/Deshabilitación de Interfaces	Exigido
Búsqueda de referencias de objetos	Exigido
Interfaz de usuario de alta resolución Capacidad de ampliación de Interfaces	Exigido
Soporte para la instalación de Azure Single Arm	Exigido
Alta disponibilidad y conmutación por error de las rutas dinámicas	Exigido
Copia de seguridad y restauración «de cualquier puerto a cualquier puerto», incluido el asistente de asignación de puertos	Exigido

	Auténtica instalación tipo Zero-Touch sin necesidad de usar una unidad flash USB	Exigido
	Referencia de objetos expandida que proporciona una mayor visibilidad de las referencias de objetos de red (uso) para interfaces, zonas, puertas de enlace y perfiles SD-WAN.	Exigido
	Ofrece compatibilidad con la API XML para recuperar recuentos de referencia (uso) de objetos, lo que ofrece visibilidad de los objetos no utilizados.	Exigido
	Soporte a certificados "Let's Encrypt"	Exigido
Administración central del Firewall	Admiistración y Reportería basada en nube para varios firewalls ofreciendo gestión de políticas de grupos de Firewalls y una única consola para todos sus productos de seguridad del fabricante	Exigido
	La administración de políticas de grupo permite que los objetos, la configuración y las políticas se modifiquen una vez y se sincronicen automáticamente en todos los firewalls del grupo	Exigido
	El Administrador de tareas proporciona una traza de auditoría histórica completa y una supervisión del estado de los cambios en las políticas de grupo	Exigido
	Administración de copias de seguridad del firmware, que almacena los cinco últimos archivos de copia de seguridad de la configuración de cada firewall, con uno que se puede anclar para su almacenamiento permanente y fácil acceso	Exigido
	Actualizaciones de firmware que ofrecen actualizaciones de firmware con un solo clic para aplicarlas a cualquier dispositivo	Exigido
	El despliegue sin intervención (Zero-touch) permite realizar la configuración inicial en la gestión basada en nube y luego exportarla para cargarla en el dispositivo desde una unidad flash al iniciarlo, conectando automáticamente el dispositivo a la consola central de administración	Exigido
	Gestión centralizada de grupos de firewalls mediante consola o panel de administración para múltiples dispositivos, con control de acceso y trazabilidad de cambios.	Exigido

	Programación de actualizaciones de firmware	Exigido
	Informes de varios firewalls por medio de los grupos de firewall	Exigido
	Guarde, programe y exporte informes desde la consola Central de administracion en Nube	Exigido
Firewall, Conexión a Redes & Enrrutamiento	Inspección profunda de paquetes de estado de Firewall (Stateful inspection)	Exigido
	Arquitectura de procesamiento de paquetes que proporciona niveles extremos de visibilidad, protección y rendimiento mediante el procesamiento de paquetes basado en flujos	Exigido
	Inspección TLS de alto rendimiento, compatibilidad con TLS 1.3 sin necesidad de downgrade, agnóstico de puertos, políticas de nivel Enterprise, visibilidad única en el panel de control y resolución de problemas de compatibilidad	Exigido
	Motor DPI que proporciona protección de escaneado de flujo para IPS, AV, Web, App Control e inspección TLS en un único motor de alto rendimiento.	Exigido
	La solución perimetral deberá contar con arquitectura de aceleración por hardware para procesamiento de tráfico, capacidad de inspección profunda de paquetes con cifrado TLS 1.3 sin degradación del throughput nominal estipulado y mecanismos de compartición de telemetría e integración con otros componentes de red mediante protocolos estándar (Syslog, CEF) o APIs REST abiertas.	Exigido
	Aceleración inteligente y basada en políticas del tráfico de confianza mediante mecanismos de procesamiento optimizado por hardware o equivalentes.	Exigido
	Aceleración e inspección del tráfico cifrado TLS, incluyendo TLS 1.3, sin necesidad de downgrade y sin degradación del throughput nominal estipulado.	Exigido
	Delegación de prefijo DHCP IPv6	Exigido
	soporte a BGPv6	Exigido

Balanceo de enlaces SD-WAN: múltiples conexiones a Internet, comprobación automática del estado de los enlaces, conmutación automática por error, balanceo automático y ponderado, y reglas granulares multitrayectoria	Exigido
Políticas basadas en usuarios, grupos, tiempo o red	Exigido
Políticas de tiempo de acceso por usuario/grupo	Exigido
Aplicación de políticas en zonas, redes o por tipo de servicio	Exigido
Aislamiento de zonas y apoyo a políticas basadas en zonas	Exigido
Zonas por defecto para LAN, WAN, DMZ, LOCAL, VPN y WiFi	Exigido
personalización de zonas para LAN o DMZ	Exigido
Políticas NAT personalizables con enmascaramiento de IP y compatibilidad total con objetos para redirigir o reenviar varios servicios en una sola regla con un práctico asistente de reglas NAT para crear rápida y fácilmente reglas NAT complejas en unos pocos pasos	Exigido
Definiciones de objetos de red reutilizables para todas las reglas con búsqueda inteligente global de texto libre	Exigido
Optimización del tráfico en configuraciones de alta disponibilidad activo-pasivo mediante mecanismos de aceleración equivalentes y tecnológicamente neutrales.	Exigido
Lista de excepciones preempaquetada	Exigido
Cubrimiento para todos los puertos/protocolos	Exigido
Soporta a todas las suites de cifrado modernas	Exigido
Visibilidad y gestión de errores	Exigido
Soporte de VLAN completo	Exigido

Aislamiento de zonas y VLAN y compatibilidad con políticas basadas en zonas	Exigido
Microsegmentación y auto aislamiento por medio de la Seguridad Sincronizada.	Exigido
Protección contra inundaciones (Flood Portection): Bloqueo DoS, DDoS y escaneo de puertos (portscan)	Exigido
Bloqueo de países por geo-IP	Exigido
Enrrutamiento Avanzado: multicast (PIM-SM), y dinamico: RIP, BGP, OSPFv3 (IPv6), BGP6 con soporte completo 802.1Q VLAN	Exigido
Soporte de Upstream Proxy	Exigido
Protocolo de enrrutamiento independiente con IGMP snooping	Exigido
Bridging con soporte STP y ARP broadcast forwarding	Exigido
soporte a VLAN DHCP y tagging	Exigido
soporte a VLAN bridge	Exigido
Soporte a Jumbo Frame	Exigido
Soporte a Wireless WAN (no aplica para implementaciones virtuales)	Exigido
802.3ad interface link aggregation	Exigido
Configuración completa a DNS, DHCP y NTP	Exigido
Dynamic DNS (DDNS)	Exigido
Soporte a IPv6	Exigido
Certificación IPv6 Ready Logo Program Approval	Exigido

	Delegación IPv6 DHCP Prefix	Exigido
	soporte a IPv6 tunnelling incluyendo 6in4, 6to4, 4in6, y IPv6 implementación rápida (6rd) por medio de IPSec	Exigido
	Soporte 5G: Permite la conectividad celular 5G mediante las bandas 5G sub-6 GHz, con una velocidad máxima de descarga de hasta 4,5 Gbps.	Exigido
	New option to redistribute BGP routes into OSPFv3	Exigido
	Puede clonar rutas estáticas, activarlas o desactivarlas y añadir descripciones. El firewall ofrece una opción de ruta blackhole. También admite Equal-Cost Multi-Path (ECMP) para equilibrar la carga.	Exigido
	Soporte NAT64	Exigido
SD-WAN	Integración de SD-WAN de terceros con redes troncales de Cloudflare, Akamai y Azure	Exigido
	Escalabilidad de gateways de SD-WAN	Exigido
	Balanceo de Cargas de SD-WAN	Exigido
	Enrutamiento dinámico con OSPFv3 (IPv6)	Exigido
	Perfiles de SD-WAN con soporte a múltiples canales WAN incluyendo VDSL, DSL, cable, LTE/celular y MPLS.	Exigido
	SLAs basados en rendimiento que automáticamente seleccionen el mejor enlace WAN en función de Jitter, Latencia o pérdida de paquetes.	Exigido
	Impacto-Zero mantiene el redireccionamiento de las sesiones de las aplicaciones cuando el rendimiento del enlace cae por debajo de los umbrales y se realice una transición a un enlace WAN de mejor desempeño	Exigido
	Los gráficos de monitoreo de SD-WAN deben proporcionar información en tiempo real sobre latencia, Jitter y pérdida de paquetes para todos los enlaces WAN configurados.	Exigido

	Aceleración por hardware o mecanismo equivalente del tráfico de túneles IPsec utilizado por funciones SD-WAN.	Exigido
	Selección y enrutamiento de rutas de aplicación, que se utiliza para garantizar la calidad y minimizar la latencia para aplicaciones de misión crítica como VoIP	Exigido
	SD-WAN con intercambio de telemetría y contexto de aplicaciones entre componentes de seguridad y endpoints mediante protocolos estándar (Syslog, CEF) o APIs REST abiertas, para mejorar la identificación de aplicaciones y la aplicación dinámica de políticas.	Exigido
	Enrutamiento sincronizado de aplicaciones SD-WAN a través de enlaces preferentes mediante reglas de firewall o enrutamiento basado en políticas.	Exigido
	Implementación abseguible, flexible y sin intervención o con intervención mínima	Exigido
	Robusta compatibilidad con VPN, incluido IPSec y VPN SSL	Exigido
	Orquestación centralizada de VPN	Exigido
	Túnel exclusivo de RED en capa 2 con enrutamiento	Exigido
	Integración con Azure Virtual WAN para una completa red superpuesta SD-WAN	Exigido
Traffic Shaping & Quotas	Tráfico flexible o modelado de tráfico (QoS)	Exigido
	Poder establecer cuotas de tráfico basadas en el usuario sobre el tráfico de carga/descarga o total y cíclico o no cíclico	Exigido
	Otimización en tiempo Real de VoIP	Exigido
	DSCP marking	Exigido
Autenticación	Identificación transparente de usuarios integrable con Active Directory o servicios de directorio equivalentes, mediante agentes, protocolos estándar o APIs, sin exigir mecanismos propietarios.	Exigido

Soportar Autenticación via: Active Directory, eDirectory, RADIUS, LDAP y TACACS+	Exigido
Agentes, protocolos o mecanismos compatibles para autenticación SSO con Active Directory o servicios de directorio equivalentes.	Exigido
Single sign-on: Active directory, eDirectory, RADIUS Accounting	Exigido
Radius Timeout con autenticación de dos factores (2FA) y (MFA)	Exigido
agentes de autenticación para Clientes Windows, Mac OS X, Linux 32/64	Exigido
Autenticación SSO de navegador: Transparente, autenticación proxy (NTLM) y Kerberos	Exigido
Portal Captivo en el Navegador	Exigido
Certificados de autenticación para iOS y Android	Exigido
Servicios de autenticación para IPSec, SSL, L2TP, PPTP	Exigido
Compatibilidad con la autenticación de Google Chromebook para entornos con Active Directory y Google G Suite	Exigido
Autenticación basada en API	Exigido
Integración con Azure AD	Exigido
Integración de Azure AD para el inicio de sesión en la consola web SSO	Exigido
SSO de Azure AD para portal cautivo	Exigido
Azure Group Import	Exigido
Azure RBAC Automático	Exigido

	Soporte para la creación de usuarios con formato UPN para autenticación RADIUS	Exigido
	Integración de Google Workspace mediante cliente LDAP y SSO de Google Chromebook	Exigido
	Capacidad de gestionar miles de solicitudes de inicio de sesión simultáneas en múltiples esquemas de SSO compatibles, incluidos mecanismos basados en agentes, RADIUS SSO u otros equivalentes.	Exigido
	Experiencia AD SSO más transparente cuando se aplica HSTS, permitiendo handshakes Kerberos y NTLM sobre HTTP o HTTPS	Exigido
Portal de Autoservicio de usuario	Poder descargar un cliente de autenticación de la marca ofertada	Exigido
	Poder descargar un cliente de acceso remoto SSL (Windows) y archivos de configuración (otros SO)	Exigido
	Información de acceso a Hotspot	Exigido
	Poder cambiar nombre de usuario y contraseña	Exigido
	Ver el uso personal de Internet	Exigido
	Acceda a mensajes en cuarentena y gestione listas de remitentes bloqueados/permitidos basadas en usuarios (requiere add-on de licencia Email Protection)	Exigido
Opciones base de VPN	Contar con un portal de VPN	Exigido
	Conmutación de conexiones IPSec por el HA	Exigido
	Soporte de host FQDN para SSLVPN	Exigido
	Monitoreo del estado del túnel VPN IPsec vía SNMP	Exigido
	Soporte de puerta de enlace remota múltiple 0.0.0.0 (=*/ ANY) para RBVPN	Exigido

Soporte PSK único	Exigido
soporte para VPNs Ipsec con DH Group 27-30 / RFC6954	Exigido
Soporte a tuneles IPsec y VPN SSL	Exigido
Orquestación de VPNs mediante un asistente guiado	Exigido
Soporte de VPNs Sitio a Sitio (Site-to-Site): SSL, IPsec, 256-bit AES/3DES, PFS, RSA, Certificados X.509, pre-shared key	Exigido
Tuneles de VPNs sitio a sitio por medio (RED) Remote Ethernet Device (Robusto y ligero)	Exigido
Aceleración por hardware o mecanismo equivalente del tráfico de túneles IPsec, tanto sitio a sitio como de acceso remoto.	Exigido
Herramientas de importar, monitorear y administrar VPC en AWS	Exigido
Soporte de conjuntos de cifrado GCM y Suite-B para IPsec	Exigido
Soporte de configuración de un tiempo de "rekey" personalizado para evitar los avisos regulares de MFA cada cuatro horas.	Exigido
Soporte de la definición de selectores de tráfico dentro de una RBVPN específica, que sólo permite el tráfico a través del túnel si el tráfico coincide con el par especificado de direcciones locales y remotas.	Exigido
Soporte a L2TP y PPTP	Exigido
VPN basadas en enrutamiento	Exigido
Soporte de Clientes de VPNs tipo Remote access para: SSL, IPsec, iPhone/iPad/ Cisco/Andriod	Exigido
Soporte a IKEv2	Exigido

	Cliente SSL para Windows y descarga de la configuración a través del portal de usuario	Exigido
	Soporte por defecto de TLS 1.3 en túneles SSL VPN	Exigido
	Soporte de cifrado GCM para VPN SSL	Exigido
	Opción masiva para activar y desactivar conexiones VPN IPSec de sitio a sitio	Exigido
	Filtrado de interfaces XFRM	Exigido
	Retransmisión DHCP a través de interfaces XFRM a servidores DHCP desplegados detrás del firewall	Exigido
Cliente de VPN	Soporte para VPNs IPSec y SSL	Exigido
	Aprovisionamiento e implementación sencilla	Exigido
	Gratuito (licencias ilimitadas de acceso remoto SSL incluidas sin costo adicional)	Exigido
	Autenticación: Pre-Shared Key (PSK), PKI (X.509), Token y XAUTH	Exigido
	Capacidad de intercambiar telemetría de postura de seguridad entre el firewall y los endpoints conectados remotamente, mediante mecanismos abiertos, APIs o integraciones equivalentes.	Exigido
	Split-tunneling inteligente para un enrutamiento óptimo del tráfico	Exigido
	Soporte a NAT-traversal	Exigido
	"Client-monitor" para una visión gráfica del estado de la conexión	Exigido
	Soporte para Mac y Windows	Exigido

	Aprovisionamiento de políticas IPSec de acceso remoto con el cliente.	Exigido
	Compatibilidad de grupos que permite importar desde AD/LDAP, etc.	Exigido
	Conexión automática para remote access en IPSec y SSL VPN	Exigido
Intrusion Prevention System (IPS)	Motor de inspección profunda de paquetes IPS de próxima generación y alto rendimiento con patrones IPS selectivos que se pueden aplicar sobre la base de reglas de firewall para obtener el máximo rendimiento y protección	Exigido
	Interruptor IPS global para activar o desactivar la funcionalidad de IPS	Exigido
	Protección contra amenazas de día cero	Exigido
	Defensas Perimetrales	Exigido
	Contar con miles de Firmas	Exigido
	Selección granular de categorías	Exigido
	Soporte para firmas IPS personalizadas	Exigido
	Los filtros inteligentes de políticas IPS permiten políticas dinámicas que se actualizan automáticamente a medida que se añaden nuevos patrones	Exigido
Respuesta automatizada a amenazas e integración de seguridad	Respuesta automatizada frente a amenazas avanzadas y comunicaciones con destinos maliciosos, con capacidad de supervisar, bloquear y contener eventos identificados mediante DNS, IPS, fuentes de inteligencia y otros motores de seguridad integrados.	Exigido
	Respuesta automatizada frente a amenazas identificadas por fuentes de inteligencia, plataformas MDR/XDR, analistas SOC o fuentes autorizadas de terceros.	Exigido

	Respuesta automatizada frente a amenazas provenientes de fuentes de inteligencia del sector, verticales o regionales, mediante mecanismos de integración abiertos o equivalentes.	Exigido
	La solución deberá identificar y marcar los dispositivos comprometidos que intenten comunicarse con indicadores de amenaza, compartiendo telemetría relevante del host, usuario, proceso, incidentes y hora del evento con los componentes de seguridad integrados.	Exigido
	Las condiciones de seguridad podrán asociarse a reglas de firewall para limitar automáticamente el acceso a recursos y segmentos de red de un dispositivo comprometido hasta su remediación.	Exigido
	La solución deberá permitir activar automáticamente mecanismos de contención contra movimiento lateral cuando un endpoint gestionado resulte comprometido, restringiendo su comunicación con otros recursos, incluso dentro del mismo segmento LAN.	Exigido
	Políticas de firewall dinámicas basadas en contexto y estado de seguridad.	Exigido
	Protección multicapa frente a comunicaciones salientes hacia infraestructuras maliciosas o de comando y control.	Exigido
VPN sin cliente	La solución deberá permitir a los usuarios acceder al portal de autoservicio HTML5 cifrado único con soporte para RDP, SSH, Telnet y VNC.	Exigido
Características de protección web	Proxy totalmente transparente para antimalware y filtrado web	Exigido
	Autenticación por conexión para varios usuarios con la misma dirección IP de origen	Exigido
	Aplicación de restricciones de tenant para O365	Exigido
	Soporte de encabezado X-Forwarded-For para balanceadores de carga de flujo ascendente y proxies	Exigido
	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 OEM Labs	Exigido
Políticas de tiempo de cuota de navegación por usuario/grupo	Exigido
Políticas de acceso por tiempo para usuario/grupo	Exigido
Análisis de malware: bloquee 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 JavaScript	Exigido
Live Protection búsquedas en tiempo real en la nube para la última inteligencia de amenazas	Exigido
Segundo motor de detección de malware independiente (Avira) para el doble análisis	Exigido
Escaneo en tiempo real o en modo por lotes	Exigido
Protección de Pharming	Exigido
Análisis HTTP y HTTPS por usuario o política de red con reglas y excepciones personalizables	Exigido
Detección y refuerzo de túneles de protocolo SSL	Exigido
Validación de Certificados	Exigido
Almacenamiento en caché de contenido web de alto rendimiento	Exigido
Almacenamiento en caché forzado para actualizaciones	Exigido
Filtrado de tipos de archivo por tipo de mime, extensión y tipos de contenido activo (por ejemplo, Activex, applets, cookies, etc.)	Exigido

	Aplicación de YouTube for Schools por política (usuario/grupo)	Exigido
	Soporte de SafeSearch (basada en DNS) para los principales motores de búsqueda por política (usuario/grupo)	Exigido
	Monitoreo y aplicación de palabras clave web para registrar, informar o bloquear palabras clave coincidentes con contenido web listas con la opción de subir listas personalizadas	Exigido
	Bloquear aplicaciones potencialmente no deseadas (PUAs)	Exigido
	Opción de anulación de la política web para que los administradores o el personal se le permita temporalmente el acceso a sitios o categorías bloqueados, totalmente personalizable y gestionable por usuarios seleccionados.	Exigido
	Aplicación de políticas de usuario/grupo en Google Chromebooks	Exigido
	Filtrado web automático de sitios identificados por Internet Watch Foundation (IWF) que contienen abuso sexual infantil	Exigido
	IPv6 a IPv4 mediante proxy explícito	Exigido
	Reducción de la carga del sistema al aplicar SafeSearch, restricciones de YouTube, restricciones de dominio de inicio de sesión de Google App y restricciones de tenents de Azure AD.	Exigido
Visibilidad de Aplicaciones en la Nube	El widget Centro de control muestra la cantidad de datos cargados y descargados en aplicaciones en la nube categorizados como nuevos, sancionados, no autorizados o tolerados	Exigido
	Poder descubrir Shadow IT en un vistazo	Exigido
	Desglose para obtener detalles sobre los usuarios, el tráfico y los datos	Exigido
	Acceso con un solo clic a las políticas de modelado del tráfico	Exigido

	Filtrar el uso de aplicaciones en la nube por categoría o volumen	Exigido
	Informe detallado de uso de aplicaciones en la nube personalizable para obtener informes históricos completos	Exigido
Protección y control de aplicaciones	Control sincronizado de aplicaciones para identificar, clasificar y controlar automáticamente todas las aplicaciones desconocidas de Windows y Mac en la red compartiendo información entre los terminales gestionados y el firewall.	Exigido
	Control de aplicaciones basado en firmas con patrones para miles de aplicaciones	Exigido
	Visibilidad y control de aplicaciones en la nube para descubrir Shadow IT	Exigido
	Filtros inteligentes de control de aplicaciones que permiten políticas dinámicas que se actualizan automáticamente a medida que se añaden nuevos patrones.	Exigido
	Descubrimiento y control de microaplicaciones	Exigido
	Control de aplicaciones basado en categorías, características (por ejemplo, consumo de ancho de banda y productividad), tecnología (por ejemplo, P2P) y nivel de riesgo	Exigido
	Aplicación de políticas de control de aplicaciones por usuario o regla de red	Exigido
	Opción de limpieza automática de aplicaciones descubiertas con más de un mes de antigüedad	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
Proteccion Firewall de Aplicaciones Web	Proxy Reverso	Exigido
	Motor de refuerzo de URL con prevención de enlaces profundos y cruce de directorios	Exigido

Motor de protección de formularios	Exigido
Endurecimiento de URL estáticas	Exigido
Protección contra inyección de SQL	Exigido
Protección contra Cross-site scripting	Exigido
Debe contar con un motor de antivirus Dual	Exigido
Descarga de cifrado HTTPS (TLS/SSL)	Exigido
Firma de cookies con firmas digitales	Exigido
Enrutamiento Path-based	Exigido
Control de la políticas por Geo IP	Exigido
Configuración personalizada de cifrado y ajustes de versión TLS	Exigido
Aplicación de HSTS y X-Content-Type-Options	Exigido
Soporte del protocolo Outlook en cualquier lugar (Outlook anywhere)	Exigido
Autenticación inversa (descarga) para la autenticación básica y basada en formularios para el acceso al servidor	Exigido
Abstracción de servidor virtual y servidor físico	Exigido
El balanceador de carga integrado reparte los accesos entre varios servidores	Exigido
Omisión de comprobaciones individuales de forma granular según sea necesario	Exigido
Coincidencia de solicitudes de redes de origen o URL de destino especificadas	Exigido

Soporte para operadores lógicos y/o (and/or)	Exigido
Asistencia a la compatibilidad con diversas configuraciones e implementaciones no estándar	Exigido
Opciones para cambiar los parámetros de rendimiento de Web Application Firewall (WAF)	Exigido
Opción de límite de tamaño de escaneo	Exigido
Bloqueo de contenidos no escaneables	Exigido
Permitir/Bloquear rangos IP	Exigido
Bloqueo de clientes con mala reputación	Exigido
Filtro de amenazas comunes personalizable	Exigido
Realiza estrictos controles de seguridad de las solicitudes, como los intentos de atravesar rutas prohibidas.	Exigido
Control del protocolo	Exigido
Verifica los patrones de uso característicos de bots y crawlers.	Exigido
Impide que los servidores web filtren información al cliente. Esto incluye los mensajes de error enviados por los servidores, que los atacantes pueden utilizar para recopilar información sensible o detectar vulnerabilidades específicas.	Exigido
Políticas de Autenticación	Exigido
Plantillas de autenticación personalizables	Exigido
Protección HTTP lento	Exigido
Soporte de comodines para rutas de servidor y dominios	Exigido
Añadir automáticamente un prefijo/sufijo para la autenticación	Exigido

Logging y Reportería	Informes predefinidos con opciones de personalización flexibles	Exigido
	Informes para firewalls en (hardware, software, virtuales y en la nube)	Exigido
	Interfaz de usuario intuitiva que ofrece una representación gráfica de los datos	Exigido
	Dashboard de informes que ofrece una vista rápida de los eventos de las últimas 24 horas.	Exigido
	Identifique fácilmente las actividades de la red, las tendencias y los posibles ataques	Exigido
	Fácil copia de seguridad de los registros con rápida recuperación para necesidades de auditorías	Exigido
	Implementación simplificada sin necesidad de conocimientos técnicos	Exigido
	Cree informes personalizados con potentes herramientas de visualización	Exigido
	Búsqueda y visualización de Syslog	Exigido
	Almacenamiento de datos Syslog	Exigido
	Informes a demanda	Exigido
	Almacenamiento en la nube de 7 días para informes de Central Firewall	Exigido
	Nuevo informe de aplicaciones en la nube (CASB)	Exigido
	Reportes sin costo adicional	Exigido
Reportería On-Box	Sin costo adicional	Exigido

	La solución deberá disponer de reportes integrados y personalizables sobre tráfico, seguridad, aplicaciones, búsquedas, servidores, IPS, protección avanzada contra amenazas, estado de seguridad de endpoints, análisis de archivos/sandboxing, VPN, correo electrónico y marcos de cumplimiento aplicables.	Exigido
	Almacenamiento local o integrado en el equipo para conservar datos de registro destinados a informes históricos, sin exigir una arquitectura o denominación comercial específica.	Exigido
	Información de enrutamiento SD-WAN en los registros del firewall y también proporciona comprobaciones de estado y eventos de cambio de ruta	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
	Anonimización de informes	Exigido
	Programación de informes a varios destinatarios por grupo de informes con opciones de frecuencia flexibles	Exigido
	Exportar informes como HTML, PDF, Excel (XLS)	Exigido
	Marcadores de informes	Exigido
	Personalización de la retención de registros por categoría	Exigido
	Soporte de Syslog	Exigido
	Visor de registros en vivo con todas las funciones con vista de columna y vista detallada con potentes opciones de filtro y búsqueda, ID de regla con hipervínculos y personalización de la vista de datos	Exigido
Garantía	Garantía del Fabricante de 36 meses	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
Otras Características	Los Firewalls deberán contar con licencia mínima de 36 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
Autorización del Fabricante	El Oferente deberá contar con la Autorización del Fabricante del equipo ofertado. Deberá estar dirigida al convocante con los datos de este llamado.	Exigido

APs Wifi 6

Perfil de uso MITIC seleccionado: AP-001-01 Access Point para Redes LAN inalámbricas de escala pequeña, mediana o grande.

ITEM	ESPECIFICACIONES TÉCNICAS	CARACTERÍSTICAS	MÍNIMO EXIGIDO
1	Marca	Especificar	Exigido
2	Modelo	Especificar	Exigido
3	Número de Parte del Fabricante del / Equipo	No se requiere	No se requiere

4	Origen / Procedencia	Especificar	Exigido
5	Cantidad	40 (cuarenta) unidades	Exigido
6	Estándares de Interfaces de Radio	IEEE 802.11a/b/g/n/ac/ax.	Exigido
7	Estándares de Interfaces de Uplink	1 puerto 100/1000/2500Base-T RJ45.	Exigido
8	Entorno de Despliegue	No se requiere	No se requiere
9	Radio	3 radios: 1x 2,4 GHz; 1x 5 GHz; 1x 6 GHz.	Exigido
10	Antenas	Antenas internas.	Exigido
11	Capacidad de las Radio / Throughput	Throughput máximo: ≥ 1.000 Mbps en 2,4 GHz; ≥ 2.300 Mbps en 5 GHz; ≥ 4.600 Mbps en 6 GHz.	Exigido
12	MIMO	No se requiere	No se requiere
13	Resource Units (RUs)	No se requiere	No se requiere
14	Modos de Funcionamiento	No se requiere	No se requiere
15	Redes WLAN	48 SSID como mínimo.	Exigido
16	Conexiones Concurrentes	No se requiere	No se requiere
17	Puertos de Uplink	1 puerto de uplink 100/1000/2500Base-T RJ45.	Exigido
18	PoE	IEEE 802.3at (PoE+).	Exigido

19	Puertos RJ45	1 puerto RJ45 100/1000/2500Base-T.	Exigido
20	Otros Puertos	No se requiere	No se requiere
21	Roaming	No se requiere	No se requiere
22	VLANs	No se requiere	No se requiere
23	Potencia de Transmisión	No se requiere	No se requiere
24	Funciones de Nivel Físico y Enlace	No se requiere	No se requiere
25	Protección Física	No se requiere	No se requiere
26	Detección de Dispositivos	No se requiere	No se requiere
27	Calidad de Servicio (QoS)	No se requiere	No se requiere
28	Indicadores	No se requiere	No se requiere
29	Autoconfiguración	No se requiere	No se requiere
30	Autenticación	El dispositivo deberá soportar al menos uno de los siguientes esquemas de autenticación: WPA, WPA2, WPA3, WEP, IEEE 802.1X o Portal Cautivo.	Exigido
31	Seguridad	No se requiere	No se requiere
32	Funciones Avanzadas	No se requiere	No se requiere
33	IoT-Ready	No se requiere	No se requiere

34	Administración / Controlador	Administración, configuración, monitoreo y supervisión centralizados mediante la plataforma licenciada.	Exigido
35	Coexistencia / Optimización	No se requiere	No se requiere
36	Eficiencia Energética	No se requiere	No se requiere
37	Condiciones de Operación	No se requiere	No se requiere
38	Mantenimiento	No se requiere	No se requiere
39	Alimentación Eléctrica	Deberá incluir inyector PoE+ IEEE 802.3at para alimentación del equipo y utilización futura con infraestructura PoE.	Exigido
40	Redundancias	No se requiere	No se requiere
41	Software	Licencia por treinta y seis (36) meses que permita la administración centralizada, monitoreo y supervisión avanzada del equipo. La licencia deberá mantenerse vigente durante el mismo periodo de la garantía.	Exigido
42	Certificaciones	CE, UL, CB, FCC y EN 60601-1-2. El Oferente deberá contar con Autorización del Fabricante del equipo ofertado, dirigida al MTESS y con referencia al presente llamado.	Exigido
43	Kit de Montaje	No se requiere	No se requiere
44	Montaje e Instalación	El oferente deberá entregar, instalar y configurar el equipo de acuerdo con las indicaciones y a lo definido por la DGTIC.	Exigido
45	Documentación	No se requiere	No se requiere
46	Garantía	Garantía mínima de treinta y seis (36) meses.	Exigido
47	Ciclo de Vida	No se requiere	No se requiere

Especificación	Descripción	Exigencia
Detalle	Marca:	Especificar.
	Modelo:	Especificar.
	Procedencia:	Especificar.
	Cantidad:	1
Características Generales.	El equipo deberá contar con diseño modular y permitir la incorporación de tarjetas o módulos de expansión.	Exigido.
	Deberá soportar, como mínimo, 250 usuarios en su configuración base y permitir la ampliación de su capacidad hasta alcanzar, como mínimo, 450 usuarios mediante la incorporación de tarjetas de expansión.	Exigido.
	Deberá soportar, como mínimo, 50 llamadas concurrentes en su configuración base y permitir su ampliación hasta alcanzar, como mínimo, 110 llamadas concurrentes.	Exigido.
	Deberá soportar, como mínimo, 250 extensiones SIP vinculadas en su configuración base y permitir la ampliación de su capacidad hasta alcanzar, como mínimo, 450 extensiones SIP.	Exigido.
	Deberá contar con una memoria RAM de al menos 4 GB.	Exigido.
Parámetro de Video	Deberá soportar, como mínimo, los códecs de video VP8, H.263, H.263P, H.264 y MPEG-4.	Exigido.
Parámetro de Audio	Deberá soportar, como mínimo, los códecs de audio G.711 A-law/μ-law, G.722, G.726, G.729A, GSM, Speex, ADPCM e iLBC.	Exigido.
Protocolos de Red	Deberá soportar, como mínimo, los protocolos UDP, TCP, TLS y SRTP.	Exigido.
Métodos DTMF	Deberá soportar como mínimo DRMF In-band, RFC 4733, RFC 2833 y SIP Info	Exigido.
Métodos de señalización DTMF	Deberá soportar, como mínimo, los métodos de señalización DTMF In-band, RFC 4733, RFC 2833 y SIP INFO.	Exigido.

Interfaces	Deberá disponer de dos interfaces Ethernet 10/100/1000 Mbps. Como mínimo: una interfaz LAN y una interfaz WAN.	Exigido.
	Deberá incluir como mínimo una interfaz USB 2.0	Exigido.
Puertos GSM/3G/4G	Deberá soportar módulos GSM, 3G o 4G y permitir una capacidad máxima de al menos 6 puertos.	Exigido.
Puertos RJ11	Deberá permitir la incorporación de placas de expansión con hasta 8 puertos RJ11 por placa.	Exigido.
Módulos FXO, FXS	Deberá admitir módulos o placas de expansión con al menos 1 puerto de FXO y FXS	Exigido.
Garantía	Mínimo 36 meses de garantía.	Exigido.
Autorización del Fabricante	El Oferente deberá contar con la Autorización del Fabricante del equipo ofertado. Deberá estar dirigida al convocante con los datos de este llamado.	Exigido.

Condiciones

La central telefónica IP se entregará configurada de forma segura, cumpliendo como mínimo:

- a) Señalización SIP sobre TLS 1.2 o superior y media cifrada mediante SRTP, habilitadas y activas en producción para la totalidad de las extensiones que lo soporten. Las extensiones cuyo terminal no soporte cifrado se declararán en un registro de excepciones justificado y se ubicarán en un segmento diferenciado.
- b) Interfaz de administración no expuesta a Internet, accesible únicamente desde la VLAN de administración, con HTTPS y autenticación multifactor.
- c) Contraseñas de extensión de longitud mínima de doce (12) caracteres, generadas aleatoriamente y distintas del número de extensión.
- d) Bloqueo automático de direcciones IP tras cinco (5) intentos fallidos de registro en sesenta (60) segundos, con duración mínima de bloqueo de treinta (30) minutos.
- e) Restricción de llamadas salientes por perfil: los destinos internacionales, satelitales y de tarificación especial quedarán denegados por defecto y se habilitarán únicamente a las extensiones que la Convocante autorice por escrito.
- f) Límite de llamadas concurrentes salientes hacia la troncal y alerta automática ante desvíos de patrón de consumo.
- g) Registro de detalle de llamadas (CDR) conservado por doce (12) meses, exportable y enviado a la plataforma de recolección centralizada de logs.

h) Eliminación de extensiones y cuentas de demostración creadas por defecto.

Cableado Estructurado

N°	Descripción	Características Mínimas	Exigencia
		Cable de Red	
1	Marca:	Especificar fabricante.	Exigido
2	Modelo	Especificar modelo y código de fabricante.	Exigido
3	Procedencia	Especificar país de fabricación del lote ofertado.	Exigido
4	Tipo de Cable	Cable horizontal categoría 6A, F/UTP (blindado), para interior, 4 pares trenzados.	Exigido
5	Estructura	Conductores: Ocho conductores sólidos de cobre desnudo, reunidos en 4 pares trenzados.	Exigido
6		Separador interno: Debe incorporar separador central o aislador que mantenga la geometría de los pares.	Exigido
7		Cubierta: Cubierta LSZH (baja emisión de humo y libre de halógenos), continua, uniforme y sin porosidades visibles.	Exigido
8		Blindaje: Pantalla general de aluminio/poliéster y conductor de drenaje sólido.	Exigido
9		Presentación: Carrete de longitud nominal 305m	Exigido
10	Información Técnica	Número de pares: 4 pares.	Exigido
11		Calibre del conductor: 23 AWG. como mínimo	Exigido

12		Calibre de drenaje: Declarar calibre del conductor de drenaje.	Exigido
13		Diametro externo: Declarar diámetro externo nominal para cálculo de ocupación de ductos.	Exigido
14	Características eléctricas	Resistencia DC máxima: $\leq 7,8 \text{ ohm}/100 \text{ m}$.	Exigido
15		Impedencia características: $100 \text{ ohm} \pm 15 \text{ ohm}$.	Exigido
16		Delay skew: $\leq 45 \text{ ns}$.	Exigido
17		Rigidez dieléctrica: Mínimo $1500 \text{ Vac} / 2500 \text{ Vdc}$.	Exigido
18		Capacitancia mutua: $5,6 \text{ nF}/100 \text{ m} @ 500 \text{ MHz}$ o mejor.	Exigido
19		Velocidad nominal de propagación: $\text{NVP} \geq 69 \%$.	Exigido
20		Alimentación remota: Debe soportar la entrega segura de energía sobre cable LAN conforme a IEEE 802.3bt Type 4, bajo prácticas de instalación aplicables.	Exigido
21		Protocolos compatibles: 10BASE-T, 100BASE-TX, 1000BASE-T y 10GBASE-T. Se valorará soporte adicional de aplicaciones convergentes.	Exigido
22	Conformidad	Normas de Transmisión: ANSI/TIA-568.2-D o edición vigente aplicable; ISO/IEC 11801 Class EA.	Exigido
23		Reacción al fuego / LSZH: IEC 60332-1, IEC 60754-2 e IEC 61034-2, respaldadas por ficha técnica del producto ofertado.	Exigido
24		Certificación de componente: Adjuntar certificado de tercera parte o informe de ensayo de componente cuando esté disponible.	Exigido
25		Compatibilidad de sistema: El cableado, los jacks, los patch panels y los patch cords deberán ser del mismo fabricante, a fin de garantizar la compatibilidad entre todos los componentes y permitir el otorgamiento de una garantía integral del sistema de cableado estructurado.	Exigido
26		Garantía: Mínimo 3 años por defectos de fábrica. Se valorará garantía extendida de producto y aplicaciones del sistema, sujeta a condiciones del fabricante e instalación certificada.	Exigido

Conector Hembra

27	Color	Opcional	Exigido
28	Estructura	Los contactos deben estar recubiertos con 50 micro pulgadas de oro	Exigido
29		Debe ser de dos piezas, el conector y la tapa protectora del cable.	Exigido
30		El conector debe garantizar que los pares queden separados por lo que tendrá una cruceta en la tapa protectora del cable que permita el ingreso de los pares individualmente.	Exigido
31		Debe poseer un sistema de terminación que mantenga la geometría del cable y elimine el destrenzado de los pares en este proceso.	Exigido
31	Generalidades	Debe poder alojar el cable UTP de cuatro pares cat. 6A	Exigido
33		El conector debe tener la opción de reinstalación (rearmado) por lo menos en 20 ocasiones sin deteriorar su comportamiento físico.	Exigido
34		Cada conector debe ser 100% probado para asegurar su buen desempeño	Exigido
35	Compatibilidad	Debe ser de la misma marca que la conectividad.	Exigido
Patch Cord UTP Cat. 6A			
36	Color	Opcional	Exigido
37	Estructura	Los contactos de los plugs deben tener un recubrimiento de oro de 50 micro pulgadas de oro	Exigido
38		Deben estar contruidos en cable UTP de cobre multifilar y plugs modulares en cada uno de sus extremos.	Exigido
39		Los plugs deben usar un administrador integral de pares para optimizar su desempeño y consistencia al reducir el destrenzado de los pares dentro de este.	Exigido
40		El material de los plugs debe ser termoplástico.	Exigido
41		Deben poseer etiquetas donde se pueda verificar su categoría, marca y tipo de cable	Exigido
42	Generalidades	Su desempeño debe estar probado 100%	Exigido

43		Deberán ser contruidos directamente en fábrica y adicionalmente deben venir en su bolsa original de empaque.	Exigido
44	Compatibilidad	Debe ser de la misma marca que la conectividad.	Exigido

Solución Integral de Protección y Control.

N.º	Descripcion Técnica	Minimo Exigido
1	Marca:	Identificar
2	Procedencia:	Identificar
3	Cantidad:	1
4	La solución deberá corresponder a una plataforma de Gestión de Accesos Privilegiados (PAM), multilenguaje y con licencia perpetua para una instalación.	Exigido
5	La solución deberá estar licenciada para un mínimo de 10 usuarios administradores.	Exigido
6	La solución deberá permitir gestionar una cantidad ilimitada de recursos y usuarios privilegiados.	Exigido
7	La solución deberá incluir capacidad para gestionar como mínimo 25 elementos, distribuidos entre claves SSH y certificados SSL/TLS.	Exigido
8	Garantía de 36 meses, con acceso a actualizaciones, mejoras y parches de seguridad.	Exigido
9	La solución deberá permitir descubrir automáticamente recursos, cuentas privilegiadas y credenciales existentes en la infraestructura.	Exigido
10	La solución deberá permitir iniciar conexiones privilegiadas mediante RDP, SSH, VNC, SQL, HTTP y HTTPS desde una consola web centralizada.	Exigido
11	La solución deberá permitir iniciar sesiones remotas sin revelar las contraseñas privilegiadas al usuario.	Exigido

12	La solución deberá permitir conceder acceso temporal a recursos o credenciales durante un periodo previamente autorizado.	Exigido
13	La solución deberá permitir reservar credenciales privilegiadas en modalidad exclusiva, evitando su utilización simultánea por otros usuarios.	Exigido
14	La solución deberá permitir configurar flujos de solicitud y aprobación para el acceso y utilización de credenciales privilegiadas.	Exigido
15	La solución PAM deberá almacenar las credenciales e identidades privilegiadas en una bóveda cifrada mediante AES-256 y deberá ejecutar la rotación automatizada de contraseñas administrativas con una frecuencia máxima de treinta (30) días calendario o de forma inmediata tras el cierre de cada sesión privilegiada temporaria.	Exigido
16	La solución deberá permitir cambiar automáticamente una contraseña después de su utilización o liberación.	Exigido
17	La solución deberá descubrir y gestionar cuentas de servicio utilizadas en sistemas Windows.	Exigido
18	La solución deberá permitir cambiar contraseñas de cuentas de servicio y actualizar automáticamente sus dependencias compatibles.	Exigido
19	La solución deberá proporcionar mecanismos para eliminar o reducir las contraseñas embebidas en aplicaciones, scripts y conexiones a bases de datos.	Exigido
20	La solución deberá permitir que aplicaciones autorizadas recuperen credenciales de forma segura mediante API u otros mecanismos protegidos.	Exigido
21	La solución deberá permitir la elevación de privilegios Just-In-Time para cuentas locales de Windows, cuentas de dominio y sistemas Linux compatibles.	Exigido
22	Los privilegios elevados deberán concederse únicamente durante el periodo autorizado y retirarse automáticamente al finalizar dicho periodo.	Exigido
23	La solución deberá permitir supervisar y grabar sesiones privilegiadas realizadas mediante RDP, SSH, VNC, SQL y HTTPS.	Exigido
24	La solución deberá permitir a los administradores autorizados supervisar en tiempo real las sesiones privilegiadas activas.	Exigido
25	La solución deberá permitir intervenir o finalizar sesiones cuando se detecten actividades sospechosas o no autorizadas.	Exigido

26	La solución deberá permitir registrar, controlar o restringir los comandos ejecutados durante sesiones SSH.	Exigido
27	La solución deberá permitir definir reglas para autorizar, restringir o bloquear transferencias de archivos durante sesiones remotas.	Exigido
28	La solución deberá descubrir, importar, generar, asociar, rotar y retirar claves SSH utilizadas en la infraestructura.	Exigido
29	La solución deberá descubrir automáticamente e inventariar certificados SSL/TLS presentes en la infraestructura.	Exigido
30	La solución deberá gestionar el ciclo de vida de los certificados SSL/TLS, incluyendo solicitud, emisión, despliegue, renovación y revocación.	Exigido
31	La solución deberá integrarse con Microsoft Certificate Authority y con autoridades certificadoras públicas compatibles.	Exigido
32	La solución deberá generar alertas de vencimiento e identificar certificados débiles, vencidos, mal configurados o con vulnerabilidades conocidas.	Exigido
33	La solución deberá disponer de API e integrarse con plataformas SIEM, ITSM, DevOps, CI/CD, RPA y otras herramientas de seguridad compatibles.	Exigido
34	Garantía mínima de 36 (treinta y seis) meses	Exigido
Recolección centralizada de Logs		
N.º	Descripción Técnica	Mínimo Exigido
35	Marca:	Identificar
36	Procedencia:	Identificar
37	Fuentes de Log:	100
38	La solución deberá permitir la recolección centralizada de logs mediante mecanismos basados en agentes y sin agentes.	Exigido

39	La solución deberá recolectar logs provenientes de diferentes plataformas, sistemas operativos, aplicaciones, bases de datos y dispositivos de red.	Exigido
40	La solución deberá permitir importar logs históricos y configurar su importación periódica.	Exigido
41	La solución deberá recolectar eventos de Windows, mensajes Syslog y logs generados por aplicaciones personalizadas.	Exigido
42	La solución deberá contar con mecanismos de análisis personalizado e indexación para procesar formatos de logs propios o no reconocidos de forma nativa.	Exigido
43	La solución deberá permitir búsquedas avanzadas mediante operadores booleanos, comodines, agrupaciones, rangos y frases.	Exigido
44	La solución deberá permitir realizar búsquedas sobre logs indexados y logs sin procesar o Raw Logs.	Exigido
45	La solución deberá permitir guardar los resultados de las búsquedas como informes, gráficos, alertas, reglas de correlación o acciones de respuesta automática.	Exigido
46	La plataforma de gestión de registros deberá asegurar la retención continua de eventos por un periodo mínimo de doce (12) meses, manteniendo los últimos noventa (90) días en almacenamiento de alta velocidad. Podrá utilizar repositorios internos o externos compatibles.	Exigido
47	La solución deberá cifrar los logs recolectados, garantizar la sincronización horaria mediante NTP autenticado y asegurar la integridad de los registros mediante algoritmos de hashing u otros mecanismos criptográficos equivalentes, de modo a prevenir su modificación o borrado no autorizado.	Exigido
48	La solución deberá correlacionar eventos procedentes de diferentes fuentes y permitir crear reglas mediante filtros a nivel de campo.	Exigido
49	La solución deberá incluir reglas de correlación predefinidas para detectar ransomware, ataques de fuerza bruta, inyección SQL y otros patrones de ataque.	Exigido
50	La solución deberá permitir ejecutar scripts y flujos automatizados como respuesta a eventos o alertas de seguridad.	Exigido
51	La solución deberá generar alertas personalizadas y en tiempo real, incluidas alertas de correlación y cumplimiento.	Exigido
52	La solución deberá contar con gestión integrada de incidentes, permitiendo categorizar alertas, asignarlas a analistas, registrar notas y administrar su estado.	Exigido

53	La solución deberá generar informes de auditoría sobre cambios realizados en usuarios, equipos, grupos, unidades organizativas, DNS, contactos, esquema y permisos de Active Directory.	Exigido
54	La solución deberá registrar los valores anteriores y posteriores de los atributos modificados en Active Directory.	Exigido
55	La solución deberá auditar la creación, modificación, eliminación y demás cambios realizados sobre los objetos de directiva de grupo o GPO.	Exigido
56	La solución deberá analizar la superficie de ataque de Active Directory e identificar configuraciones o condiciones que puedan incrementar el nivel de riesgo.	Exigido
57	La solución deberá realizar copias de seguridad de Active Directory para los 2 controladores de dominio incluidos en el licenciamiento.	Exigido
58	La solución deberá permitir la restauración de la información respaldada de Active Directory ante eliminaciones, modificaciones no autorizadas o fallas operativas.	Exigido
59	La solución deberá generar informes sobre cambios de políticas, eventos del sistema, administración de objetos y tareas programadas en servidores Windows.	Exigido
60	La solución deberá auditar la ejecución y actividad de PowerShell en los servidores y sistemas Windows supervisados.	Exigido
61	La solución deberá registrar y generar informes sobre los periodos de actividad e inactividad de los 350 endpoints licenciados.	Exigido
62	La solución deberá identificar y auditar patrones de ataque dirigidos a los endpoints supervisados.	Exigido
63	La solución deberá auditar las cuentas locales existentes y sus actividades en los endpoints incluidos en el alcance.	Exigido
64	La solución deberá supervisar la integridad de archivos y carpetas en los 2 servidores de archivos Windows incluidos en el licenciamiento.	Exigido
65	La solución deberá generar alertas en tiempo real ante cambios críticos realizados sobre los archivos, carpetas o permisos supervisados.	Exigido
66	La solución deberá analizar los repositorios de información para identificar datos redundantes, obsoletos o triviales, optimizar el uso del almacenamiento y examinar permisos de seguridad.	Exigido

67	La solución deberá incorporar inteligencia de amenazas mediante fuentes externas y propias, admitir STIX/TAXII, YARA y AlienVault OTX, y relacionar los ataques detectados con el marco MITRE ATT&CK.	Exigido
68	Garantía mínima de 36 (treinta y seis) meses	Exigido
Prevención de Pérdida de Datos		
N.º	Descripción Técnica	Mínimo Exigido
69	Marca:	Especificar
70	Procedencia:	Especificar
71	La solución deberá corresponder a una plataforma de prevención de pérdida de datos para endpoints, bajo modalidad de suscripción anual mínimo 3 años	Exigido
72	La solución deberá estar licenciada para proteger y administrar como mínimo 500 estaciones de trabajo	Exigido
73	La solución deberá disponer de una consola centralizada para crear, administrar, aplicar y supervisar políticas de prevención de pérdida de datos.	Exigido
74	La solución deberá descubrir y clasificar información confidencial mediante expresiones regulares, palabras clave, extensiones de archivos y patrones personalizados.	Exigido
75	La solución deberá permitir identificar y proteger documentos confidenciales mediante técnicas de huellas digitales o concordancia de documentos.	Exigido
76	La solución deberá aplicar políticas de prevención de pérdida de datos considerando el contenido, el contexto, el usuario y el canal utilizado para transferir la información.	Exigido
77	La solución deberá monitorear, controlar y bloquear la transferencia de información confidencial mediante dispositivos USB y otros medios de almacenamiento removibles.	Exigido
78	La solución deberá detectar y bloquear el envío de información confidencial mediante clientes nativos de Outlook y servicios compatibles de correo web.	Exigido
79	La solución deberá monitorear y bloquear la carga de archivos confidenciales hacia aplicaciones y servicios de almacenamiento en la nube compatibles.	Exigido

80	La solución deberá controlar la transferencia de información confidencial mediante impresoras, carpetas compartidas de red, dispositivos Bluetooth y otros canales compatibles.	Exigido
81	La solución deberá permitir restringir el acceso a archivos confidenciales y bloquear su utilización mediante capturas de pantalla o portapapeles.	Exigido
82	La solución deberá identificar, monitorear y bloquear actividades sospechosas asociadas con amenazas internas o intentos de filtración de información.	Exigido
83	La solución deberá permitir gestionar falsos positivos y habilitar excepciones o anulaciones justificadas para usuarios autorizados, manteniendo su correspondiente registro.	Exigido
84	La solución deberá generar informes, análisis, alertas y notificaciones sobre incidentes, bloqueos e intentos de transferencia de información confidencial.	Exigido
85	Garantía mínima de 36 (treinta y seis) meses	Exigido
Evaluación y respuesta de eventos maliciosos		
N.º	Descripción Técnica	Mínimo Exigido
86	Marca	Especificar
87	Modelo	Especificar
88	Procedencia	Especificar
89	Cantidad	500
90	La administración deberá realizarse mediante una consola central única basada en nube y acceso web	Exigido
91	La consola deberá presentar dashboards en tiempo real con eventos, alertas y estado general de seguridad	Exigido
92	Debe poseer APIs abiertas para integración con SIEM y herramientas de terceros	Exigido
93	Debe permitir administración por grupos de usuarios y dispositivos	Exigido

94	Debe permitir sincronización con Active Directory	Exigido
95	Debe permitir perfiles y roles diferenciados para administradores	Exigido
96	Debe permitir exportación de reportes en PDF y CSV	Exigido
97	Debe registrar logs de auditoría de acciones administrativas	Exigido
98	Debe generar alertas críticas automáticas vía correo electrónico	Exigido
99	Debe soportar administración multiempresa/multisitio	Exigido
100	Debe permitir control de ancho de banda para distribución de actualizaciones	Exigido
101	La comunicación entre consola y agentes deberá utilizar HTTPS/TLS	Exigido
102	Debe proveer capacidades XDR (Extended Detection and Response)	Exigido
103	Debe correlacionar eventos de endpoints, red, correo, identidad y nube	Exigido
104	Debe contar con almacenamiento centralizado de telemetría	Exigido
105	Debe permitir búsqueda avanzada de amenazas	Exigido
106	Debe permitir investigaciones desde una sola consola	Exigido
107	Debe mapear amenazas según MITRE ATT&CK	Exigido
108	Debe recolectar telemetría de endpoints y soluciones integradas	Exigido
109	Debe detectar comportamiento sospechoso mediante IA	Exigido
110	Debe permitir análisis de causa raíz	Exigido
111	Debe mostrar línea temporal de eventos relacionados al incidente	Exigido
112	Debe priorizar amenazas según criticidad y riesgo	Exigido

113	Debe utilizar IA para análisis de amenazas	Exigido
114	Debe utilizar Machine Learning para detección avanzada	Exigido
115	Debe permitir respuestas automatizadas ante amenazas	Exigido
116	Debe generar resúmenes automáticos de incidentes	Exigido
117	Debe identificar amenazas desconocidas y día cero	Exigido
118	Debe analizar comportamiento de procesos y usuarios	Exigido
119	Debe automatizar tareas repetitivas del SOC	Exigido
120	Debe permitir aislar dispositivos comprometidos	Exigido
121	Debe permitir finalizar procesos maliciosos remotamente	Exigido
122	Debe contener ataques ransomware automáticamente	Exigido
123	Debe permitir reversión de ransomware	Exigido
124	Debe permitir ejecutar acciones remotas desde consola	Exigido
125	Debe permitir creación y seguimiento de casos	Exigido
126	Debe soportar playbooks automáticos de respuesta	Exigido
127	Debe integrarse con Microsoft Defender	Exigido
128	Debe integrarse con Microsoft Sentinel	Exigido
129	Debe integrarse con Microsoft Entra ID	Exigido
130	Debe integrarse con AWS	Exigido
131	Debe integrarse con Microsoft Azure	Exigido

132	Debe integrarse con Google Workspace	Exigido
133	Debe integrarse con soluciones de seguridad de correo	Exigido
134	Debe integrarse con plataformas SIEM	Exigido
135	Debe poseer APIs para integraciones personalizadas	Exigido
136	Debe detectar y bloquear ransomware	Exigido
137	Debe detectar malware avanzado	Exigido
138	Debe prevenir explotación de vulnerabilidades	Exigido
139	Debe detectar campañas de phishing	Exigido
140	Debe detectar amenazas día cero	Exigido
141	Debe detectar compromisos de identidad	Exigido
142	Debe monitorear servicios cloud	Exigido
143	Debe detectar amenazas en correo electrónico	Exigido
144	Debe poseer paneles ejecutivos en tiempo real	Exigido
145	Debe generar informes detallados de incidentes	Exigido
146	Debe generar reportes de cumplimiento	Exigido
147	Debe exportar reportes en PDF y CSV	Exigido
148	Debe mantener histórico de eventos e incidentes	Exigido
149	Compatible con Windows	Exigido
150	Compatible con Linux	Exigido

151	Compatible con macOS	Exigido
152	Compatible con ambientes híbridos	Exigido
153	Compatible con ambientes cloud	Exigido
154	Compatible con infraestructura on-premise	Exigido
155	Debe proteger y gestionar los correos electrónicos en la nube a través de una consola intuitiva basada en la nube, proporcionando acceso a toda la gama de productos del proveedor a través de una interfaz, incluyendo web, endpoint, móvil y servidor.	Exigido
156	Debe poder crear políticas de seguridad de correo electrónico únicas para individuos, grupos o todo el dominio.	Exigido
157	Debe tener la opción de clonar una política existente en la consola de administración.	Exigido
158	Debe proporcionar acceso administrativo a las listas de permitidos y bloqueados de los usuarios finales con la capacidad de importar, exportar, buscar, agregar y eliminar entradas directamente desde la consola de administración.	Exigido
159	Debe poder agregar descargos de responsabilidad en texto plano y HTML a los mensajes salientes que se pueden configurar a través de la política de Seguridad de Correo Electrónico en la consola de administración.	Exigido
160	Debe tener la capacidad de sincronizarse con Microsoft Active Directory.	Exigido
161	Debe tener la capacidad de sincronizarse con Microsoft Azure Active Directory.	Exigido
162	Debe poder mantener a los usuarios sincronizados automáticamente con el producto utilizando una herramienta de sincronización de Active Directory.	Exigido
163	Debe admitir completamente la actualización automática de datos de AD donde las empresas se hayan trasladado completamente a la nube.	Exigido
164	Debe admitir la sincronización de Google Directory.	Exigido
165	Debe proporcionar al administrador la capacidad de agregar manualmente buzones o importar buzones y alias cuando Active Directory no esté disponible.	Exigido

166	Debe tener actualizaciones de amenazas en vivo para detener los ataques más recientes.	Exigido
167	Debe tener detección anti-spam, antivirus y anti-phishing.	Exigido
168	Debe tener filtrado de reputación que pueda bloquear el spam.	Exigido
169	Debe tener tecnología de filtrado de reputación de próxima generación que elimine el spam de botnets a nivel de conexión IP mediante el monitoreo de solicitudes de conexión y rechace aquellas que muestren evidencia de conexiones de botnets.	Exigido
170	Debe proteger contra el spam de tipo snowshoe.	Exigido
171	Debe dar a los usuarios la capacidad de cifrar correos electrónicos usando el complemento de M365 del producto.	Exigido
172	Debe tener cifrado basado en push que proteja todo el correo electrónico o solo los archivos adjuntos.	Exigido
173	Debe tener cifrado	Exigido
174	TLS forzado que evite la interceptación cuando los mensajes están en tránsito.	Exigido
175	Debe ser capaz de añadir una firma digital para verificar la identidad del remitente con S/MIME.	Exigido
176	Debe tener un cifrado de portal web completo opcional (requiere una licencia adicional) que permita a los usuarios gestionar, leer y responder a mensajes cifrados en un portal web seguro.	Exigido
177	Debe ser capaz de personalizar la marca de su portal de cifrado y los mensajes cifrados con el logotipo y los colores de su organización (requiere una licencia adicional).	Exigido
Control estricto de usuarios remotos		
N.º	Descripción Técnica	Mínimo Exigido
178	Marca:	Identificar
179	Procedencia:	Identificar

180	La solución deberá incluir una suscripción para la protección integral del entorno de trabajo digital durante un periodo mínimo de 36 meses y para un mínimo de 50 usuarios.	Exigido
181	La solución deberá permitir administrar el navegador seguro, las políticas web, DNS Protection, ZTNA, monitoreo de correo, registros y reportes desde una consola central única o integrada nativamente.	Exigido
182	La solución deberá integrarse nativamente con la protección de endpoints y las capacidades EDR/XDR existentes, aprovechando la postura del dispositivo y la telemetría de seguridad.	Exigido
183	La solución deberá proporcionar un navegador empresarial endurecido, basado en tecnología Chromium o equivalente, administrado mediante políticas centralizadas.	Exigido
184	El navegador empresarial deberá ser compatible, como mínimo, con Windows 10 y Windows 11 de 64 bits, así como con equipos macOS basados en procesadores Intel y Apple silicon.	Exigido
185	La solución deberá permitir la instalación individual del navegador desde la consola y su despliegue masivo mediante Microsoft Intune para Windows y Jamf Pro para macOS, o herramientas equivalentes.	Exigido
186	El navegador seguro deberá recibir actualizaciones y parches de seguridad, y permitir consultar centralmente la versión instalada en los dispositivos.	Exigido
187	La solución deberá permitir crear múltiples políticas de navegación web aplicables por usuarios, grupos, aplicaciones, postura del dispositivo, sitios y categorías web.	Exigido
188	Las políticas de navegación deberán permitir ejecutar acciones de permitir, bloquear o advertir de acuerdo con el riesgo, la categoría, el sitio, la aplicación o el nivel de cumplimiento del dispositivo.	Exigido
189	La solución deberá permitir identificar y controlar el uso de aplicaciones SaaS autorizadas y no autorizadas por la organización.	Exigido
190	La solución deberá permitir exigir que el acceso a aplicaciones SaaS críticas se realice exclusivamente desde el navegador empresarial seguro, mediante integración con el proveedor de identidad o un mecanismo equivalente.	Exigido
191	La solución deberá permitir controlar o restringir acciones de copiar y pegar, impresión, capturas de pantalla, compartición de pantalla, guardado de páginas y otros intercambios de información realizados dentro del navegador.	Exigido
192	La solución deberá permitir controlar las cargas y descargas de archivos e inspeccionarlas mediante análisis de reputación y mecanismos adicionales de detección de archivos maliciosos o no confiables.	Exigido

193	La solución deberá permitir monitorear el uso de aplicaciones de inteligencia artificial basadas en web para identificar o restringir usos no autorizados.	Exigido
194	La solución deberá evaluar la postura del dispositivo antes de permitir el acceso, considerando como mínimo el sistema operativo, el estado de protección del endpoint y el cifrado del disco.	Exigido
195	La solución deberá restringir automáticamente el acceso de dispositivos comprometidos o que no cumplan las políticas de seguridad, hasta que sean remediados.	Exigido
196	La solución deberá integrarse con Microsoft Active Directory y Microsoft Entra ID, o plataformas equivalentes, para sincronizar usuarios y grupos y utilizarlos en políticas de acceso.	Exigido
197	La solución deberá incluir un servicio de DNS Protection administrado desde la consola central, que opere como resolutor DNS seguro para usuarios y endpoints.	Exigido
198	La solución deberá redirigir las consultas DNS hacia el servicio de protección mediante DNS sobre HTTPS o un mecanismo seguro equivalente.	Exigido
199	La solución deberá permitir aplicar políticas de filtrado DNS por categorías web y listas personalizadas de dominios permitidos o bloqueados, otorgando precedencia a dichas listas.	Exigido
200	La solución deberá permitir configurar exclusiones de dominios y subdominios, manejar respuestas NXDOMAIN, presentar páginas de bloqueo y generar registros y reportes de actividad DNS.	Exigido
201	La solución deberá incluir capacidades de Zero Trust Network Access para controlar el acceso a aplicaciones internas, recursos privados y entornos de nube privada según la identidad y postura del dispositivo.	Exigido
202	El servicio ZTNA deberá soportar autenticación multifactor, incluyendo OTP por correo electrónico o un mecanismo equivalente, y permitir incorporar protección CAPTCHA contra intentos automatizados.	Exigido
203	La solución deberá admitir gateways ZTNA provistos en la nube y gateways locales alojados en la infraestructura de la institución.	Exigido
204	En modalidad cloud, la solución deberá permitir seleccionar una región o punto de presencia y configurar un punto secundario con failover automático.	Exigido
205	El gateway ZTNA local deberá poder implementarse como appliance virtual sobre VMware ESXi y Microsoft Hyper-V, o plataformas equivalentes, y soportar alta disponibilidad mediante agrupación de nodos.	Exigido

206	La solución deberá permitir acceso sin agente a sesiones RDP y SSH hacia recursos internos o privados, utilizando el navegador seguro y políticas de acceso Zero Trust.	Exigido
207	La solución deberá recibir y analizar copias de correos mediante journaling compatible con Microsoft 365 o Gmail, sin modificar el mensaje original ni impedir su entrega al destinatario.	Exigido
208	La solución deberá mantener historial de mensajes, registros, cuarentena y reportes, además de permitir recuperación manual posterior a la entrega mediante integración API con Microsoft 365.	Exigido
209	La solución deberá centralizar la telemetría de navegación, DNS, ZTNA y correo; permitir consultas avanzadas y generar reportes programables, exportables como mínimo en PDF, CSV o HTML.	Exigido
210	El Oferente deberá contar con la Autorización del Fabricante del equipo ofertado. Deberá estar dirigida al convocante con los datos de este llamado.	Exigido

Acuerdo de Nivel de Servicio (SLA)

El presente Acuerdo de Nivel de Servicio será aplicable al proyecto de Cableado de Red y Equipos de Networking, incluyendo los switches core y de acceso, firewalls, puntos de acceso inalámbrico, cableado estructurado Categoría 6A, enlaces de fibra óptica y plataformas de seguridad contempladas en el pliego.

El SLA estará vigente durante el periodo de garantía, soporte técnico o suscripción correspondiente a cada ítem, contado desde la recepción final y puesta en funcionamiento de la solución.

Nivel de severidad	Descripción aplicada al proyecto	Tiempo máximo de respuesta	Tiempo máximo de solución o restablecimiento
Severidad 1 (Crítica)	Interrupción total de la red institucional; indisponibilidad simultánea de los switches core o firewalls configurados en HA; caída total de los enlaces troncales de fibra óptica; pérdida generalizada de conectividad entre pisos; indisponibilidad total del acceso a Internet o de los servicios críticos de seguridad; o falla eléctrica que provoque la interrupción total de los equipos de red.	1 hora	8 horas

Severidad 2 (Alta)	Falla de uno de los equipos que integran la configuración de alta disponibilidad; pérdida de redundancia en switches core, firewalls o enlaces troncales; interrupción de la red en uno o más pisos; falla importante del cableado o fibra que afecte a una dependencia; indisponibilidad significativa de la red inalámbrica; o afectación importante de una plataforma de seguridad, existiendo una alternativa temporal de operación.	2 horas	16 horas
Severidad 3 (Media)	Incidentes que afecten parcialmente puntos de red, puertos, patch panels, enlaces de fibra, puntos de acceso, configuraciones de switches, políticas de firewall o funcionalidades de las plataformas de seguridad, sin impedir la operación general de la institución.	3 horas	3 días hábiles
Severidad 4 (Baja)	Consultas técnicas, solicitudes de revisión o configuración, ajustes menores, actualización de diagramas o documentación, etiquetado, mantenimientos preventivos, revisión de certificaciones o incidentes sin impacto operativo significativo.	4 horas	5 días hábiles

a. Condiciones de aplicación del SLA

- Registro del incidente:** el tiempo de respuesta se contabilizará desde la recepción y registro formal del incidente por cualquiera de los canales habilitados por la convocante, tales como teléfono, correo electrónico o plataforma de gestión de tickets.
- Horario de atención:** los incidentes de severidad 1 y 2 deberán contar con atención 24 horas al día, los 7 días de la semana, y sus plazos se computarán en horas corridas. Para las severidades 3 y 4 se considerarán días y horas hábiles.
- Tiempo de respuesta:** corresponde al periodo comprendido entre el registro del incidente y el inicio efectivo de la atención por parte de personal técnico calificado.
- Tiempo de solución o restablecimiento:** comprende la recuperación del servicio mediante una solución definitiva o una medida temporal que permita restablecer la operación institucional.
- Soluciones temporales:** cuando se aplique una medida temporal, el proveedor deberá continuar con las gestiones necesarias hasta implementar la solución definitiva, sin que ello implique el cierre técnico del incidente. La solución definitiva deberá implementarse en un plazo máximo de diez (10) días hábiles contados desde el restablecimiento temporal, salvo los casos de RMA formalmente acreditados conforme al numeral siguiente, manteniéndose en todo momento la medida de contingencia.
- Fallas de hardware:** cuando la solución definitiva dependa del reemplazo de equipos o componentes mediante garantía o RMA del fabricante, el proveedor deberá implementar, siempre que resulte técnicamente posible, mecanismos de contingencia, redundancia o equipos temporales que permitan restablecer la operación.
- Atención presencial o remota:** el soporte podrá prestarse remotamente o de manera presencial, según la naturaleza del incidente y las necesidades determinadas por la convocante. Cuando la atención remota no resulte suficiente, el proveedor deberá disponer la asistencia presencial correspondiente.
- Clasificación del incidente:** la severidad inicial será establecida por la convocante considerando el alcance de la falla, los servicios afectados, la cantidad de usuarios o pisos involucrados y el impacto sobre la operación institucional.
- Atención continua:** los incidentes de severidad 1 deberán ser atendidos de manera continua hasta el restablecimiento del servicio. Los incidentes de severidad 2 también deberán recibir seguimiento continuo mientras persista una afectación relevante.
- Escalamiento:** el proveedor deberá disponer de un procedimiento de escalamiento técnico y administrativo, incluyendo la gestión con el fabricante cuando el incidente requiera soporte especializado.
- Informe de causa raíz:** para incidentes de severidad 1 y, cuando sea requerido, de severidad 2, el proveedor deberá presentar un informe de causa raíz dentro de los 3 días hábiles posteriores al restablecimiento, incluyendo las acciones correctivas y preventivas recomendadas.
- Documentación de la atención:** cada incidente deberá quedar documentado, indicando como mínimo:
 - Número o código del incidente.
 - Fecha y hora de apertura.

- Nivel de severidad asignado.
- Equipos, enlaces, pisos o servicios afectados.
- Diagnóstico realizado.
- Acciones ejecutadas.
- Fecha y hora del restablecimiento.
- Solución temporal o definitiva aplicada.
- Recomendaciones técnicas.

13. **Suspensión de plazos:** los plazos podrán suspenderse cuando la continuidad de la atención dependa de información, accesos, autorizaciones, energía eléctrica, infraestructura o condiciones bajo responsabilidad de la convocante. La suspensión deberá quedar formalmente documentada.
14. **Exclusiones:** no se considerarán incumplimientos del SLA los incidentes ocasionados por fuerza mayor, daños intencionales, intervenciones no autorizadas, fallas de servicios de terceros o condiciones externas fuera del control del proveedor, siempre que estas circunstancias sean debidamente demostradas.
15. **Cierre del incidente:** un incidente solamente podrá cerrarse una vez restablecido el servicio y obtenida la conformidad del responsable técnico designado por la convocante.

Medición y verificación del SLA: todos los tiempos se medirán a partir de las marcas de fecha y hora registradas en el ticket o medio formal de atención. Para cada incidente se documentarán, como mínimo, la hora de apertura, la primera respuesta técnica, el restablecimiento del servicio, la implementación de la solución definitiva y el cierre con conformidad del MTESS. El proveedor deberá presentar mensualmente un reporte consolidado de cumplimiento del SLA con el detalle y evidencia de cada incidente.

Unidad de incumplimiento: cada incidente constituirá una unidad independiente de medición. Existirá incumplimiento cuando el tiempo de respuesta o el tiempo de solución/restablecimiento exceda el máximo correspondiente a la severidad asignada, descontando únicamente las suspensiones formalmente documentadas. Si en un mismo incidente se incumplen ambos tiempos, se registrará un único evento de incumplimiento tomando como referencia el desvío de mayor entidad, a efectos de evitar duplicidad.

Incumplimiento reiterado: se considerará reiteración cuando se produzcan dos (2) incumplimientos de una misma severidad dentro de un periodo de treinta (30) días calendario o tres (3) incumplimientos de cualquier severidad dentro de sesenta (60) días calendario. En estos casos, el proveedor deberá presentar un plan de acción correctiva dentro de los dos (2) días hábiles siguientes a la notificación de la Convocante.

Aplicación de consecuencias contractuales: los incumplimientos verificados quedarán asentados en el registro de SLA y habilitarán la aplicación de las penalidades, multas u otras medidas previstas en el Contrato y en el Pliego de Bases y Condiciones. Cuando corresponda aplicar una penalidad contractual, la unidad de aplicación será el incidente confirmado conforme al mecanismo precedente y se vinculará al ítem o componente afectado.

b. Contactos de soporte:

El proveedor deberá designar un responsable técnico y proporcionar como mínimo:

- Nombre del responsable.
- Número telefónico de contacto.
- Correo electrónico.
- Medio de contacto para incidentes críticos.

c. Incumplimiento del SLA

El incumplimiento de los niveles de servicio será determinado y documentado conforme a los mecanismos de medición, unidad de incumplimiento y criterios de reiteración establecidos precedentemente. Los incumplimientos reiterados serán considerados incumplimiento contractual y darán lugar, cuando corresponda, a las penalidades y demás medidas previstas en el Contrato y en el Pliego de Bases y Condiciones.

Gestión de vulnerabilidades y parches críticos: durante el periodo de garantía de treinta y seis (36) meses, el proveedor deberá aplicar las actualizaciones de firmware y parches de seguridad. Ante vulnerabilidades con calificación CVSS v3.1 igual o superior a 9.0 (Crítico), el plazo máximo de parcheo o mitigación será de siete (7) días calendario desde su publicación oficial. Para vulnerabilidades de severidad Alta (CVSS 7.0 a 8.9), el plazo máximo será de quince (15) días calendario.

Condiciones de Servicio de Ciberseguridad

Ante la detección de incidentes de seguridad clasificados como Severidad 1 (Crítica) por parte de las plataformas desplegadas (EDR/XDR, Firewall, SIEM), el proveedor notificará formalmente al MTESS en un plazo máximo de dos (2) horas. El proveedor entregará un informe técnico preliminar de causa raíz y medidas de contención en un plazo no mayor a veinticuatro (24) horas, sin perjuicio del informe definitivo previsto en el SLA.

CONDICIONES GENERALES

a) Instalación y puesta en funcionamiento

El oferente será responsable de la instalación, configuración, integración y puesta en funcionamiento de la totalidad de los equipos suministrados, garantizando su correcta operatividad.

Hardening

El adjudicatario deberá realizar la configuración y puesta en marcha de la totalidad de los equipos de red, firewalls y switches aplicando los lineamientos de seguridad del CIS Benchmark Nivel 1 correspondiente. Previo a la recepción provisoria, deberá entregar un informe auditable que verifique como mínimo el cambio de credenciales por defecto, la deshabilitación de servicios no esenciales o inseguros (incluidos Telnet, HTTP, SNMPv1 y SNMPv2 cuando no resulten imprescindibles) y la activación de protocolos seguros de administración, incluyendo SSHv2, HTTPS y TLS 1.3 cuando el equipo lo soporte.

b) Soporte técnico

El oferente deberá proporcionar un servicio de soporte técnico para atender incidentes, consultas o cualquier eventualidad relacionada con la solución implementada. La asistencia podrá prestarse de manera presencial o remota, conforme a las necesidades de la entidad contratante.

c) Planificación y coordinación de los trabajos

El oferente deberá elaborar un cronograma detallado de ejecución, que contemple las actividades de implementación y los demás servicios requeridos. Dicho cronograma deberá ser coordinado con la entidad contratante. Asimismo, deberá mantener informado al responsable técnico designado sobre los avances, eventuales inconvenientes y cumplimiento de los plazos establecidos.

El oferente deberá adjuntar en su propuesta técnica un diagrama de Gantt, elaborado bajo metodología PMBOK o equivalente, con un cronograma estimado de cien (100) días distribuido en las siguientes fases: 1) Relevamiento y Diseño: 15 días; 2) Despliegue Físico en Paralelo de Cableado y Energía: 30 días; 3) Montaje, hardening e integración lógica: 20 días; 4) Pruebas de Aceptación Técnica (PAT): 10 días; 5) Migración Gradual y Puesta en Marcha: 15 días; y 6) Cierre y Capacitación: 10 días.

Previo a la puesta en marcha o conmutación final de cualquier componente crítico de red, seguridad, energía o telefonía, el MTESS deberá auditar y aprobar el Acta de Conformidad de Pruebas de Aceptación Técnica (PAT). Sin dicha aprobación formal y por escrito, no se autorizará ninguna ventana de corte o migración definitiva.

d) Capacitación

El oferente deberá impartir una capacitación con una carga horaria mínima de 30 (treinta) horas, dirigida a 2 (dos) funcionarios designados por la entidad contratante. La capacitación deberá abarcar la operación de las soluciones implementados.

e) Acompañamiento Técnico

Una vez concluidas la capacitación, la transferencia de conocimientos y la demostración de las funcionalidades de la solución, el Oferente deberá poner a disposición de la institución un banco de 150 horas de acompañamiento técnico especializado.

Estas horas podrán ser utilizadas a requerimiento de la Convocante durante un periodo de 36 meses, contado desde la recepción definitiva de la solución. La disponibilidad del banco de horas deberá acreditarse mediante una carta

compromiso en carácter de declaración jurada presentada por el Oferente.

f) Seguridad y confidencialidad de la información

La ejecución de los trabajos deberá realizarse de manera segura, ordenada y eficiente. El oferente estará obligado a mantener estricta confidencialidad respecto de los datos, documentos e informaciones a los que acceda durante la prestación del servicio, garantizando en todo momento su integridad, disponibilidad y adecuada protección.

Considerando que el adjudicatario podrá acceder a áreas restringidas e información sensible de la institución, deberá contar con una certificación vigente de un Sistema de Gestión de Seguridad de la Información, que acredite la aplicación de controles y buenas prácticas para la protección, confidencialidad e integridad de los datos.

COMPLEMENTO DE SEGURIDAD

Acceso remoto. La presente cláusula rige todo acceso remoto a los equipos, plataformas, consolas, datos o servicios comprendidos en el objeto del llamado, cualquiera sea el ítem, el canal, la etapa contractual y el sujeto que lo ejerza — Adjudicatario, subcontratistas autorizados, fabricante, usuarios institucionales y accesos no interactivos o automatizados (cuentas de servicio, integraciones por API, agentes de telemetría y flujos salientes hacia infraestructura de terceros)—. Prevalece sobre cualquier funcionalidad o requisito de las fichas técnicas que resulte incompatible.

a) Principio. Todo acceso remoto está denegado por defecto y solo se habilita de forma expresa, nominada, acotada en alcance y en tiempo, registrada y revocable unilateralmente por la Convocante. Ninguna interfaz de administración de los bienes suministrados podrá quedar alcanzable desde Internet; su cumplimiento se verificará en la Prueba de Aceptación de Seguridad.

b) Canal. Los accesos administrativos del Adjudicatario, sus subcontratistas y el fabricante se canalizarán obligatoriamente a través de la plataforma de gestión de accesos privilegiados suministrada, con credencial no revelada al operador. Los accesos de usuarios institucionales se ejercerán por el servicio de acceso Zero Trust o la VPN institucional. Quedan prohibidos: herramientas de soporte remoto de terceros no autorizadas por escrito, túneles inversos o servicios de exposición de puertos, cuentas compartidas, genéricas o de fábrica, credenciales embebidas en aplicaciones o secuencias de comandos, y el reenvío del acceso a personas no incluidas en la nómina del literal g).

c) Autorización. Requiere autorización previa y escrita del responsable técnico de la Convocante, por ventana máxima de veinticuatro (24) horas prorrogable expresamente, con revocación automática al vencimiento. Ante incidentes de Severidad 1 o 2 la habilitación podrá ser inmediata por autorización verbal, ratificada por escrito dentro de las cuatro (4) horas, con ventana máxima de doce (12) horas. Los privilegios administrativos se otorgarán bajo modalidad justo a tiempo, con retiro automático al vencimiento; no se admiten privilegios permanentes para personal externo.

d) Requisitos de la sesión. Autenticación multifactor obligatoria en todos los casos; para accesos privilegiados el segundo factor será TOTP o llave FIDO2/WebAuthn, no admitiéndose códigos por correo electrónico ni mensaje de texto. Canal cifrado con TLS 1.2 o superior, o IPsec con AES-256-GCM, SHA-256 y grupo Diffie-Hellman 19 o superior; quedan prohibidos SSLv3, TLS 1.0/1.1, 3DES, DES, RC4, MD5 y SHA-1. Evaluación de postura del dispositivo de origen (sistema operativo soportado, protección de endpoint activa, cifrado de disco). Acceso por recurso y no por red, sin enrutamiento dividido. Restricción a rangos de origen declarados. Cierre por inactividad a los quince (15) minutos. Bloqueo tras cinco (5) intentos fallidos por treinta (30) minutos. Contraseñas privilegiadas de catorce (14) caracteres mínimo, custodiadas en bóveda y rotadas automáticamente al finalizar cada uso.

e) Registro y supervisión. Grabación íntegra de toda sesión privilegiada, incluido el registro de comandos ejecutados. La Convocante podrá supervisar en tiempo real y terminar unilateralmente cualquier sesión, sin que ello genere reclamo, prórroga del Acuerdo de Nivel de Servicio ni compensación. Transferencia de archivos denegada por defecto, habilitable por sesión con registro. Retención de grabaciones y registros: doce (12) meses (aceptable 12 a 24), con los últimos noventa (90) días de consulta inmediata, cifrados, con verificación de integridad y sin posibilidad de alteración ni eliminación por el Adjudicatario, el fabricante o sus operadores. Los eventos se remitirán a la plataforma de recolección centralizada de logs, con alerta automática ante acceso fuera de ventana, origen no declarado, elevación no aprobada o transferencia no autorizada.

f) Accesos automatizados. Se ejercerán mediante cuentas de servicio nominadas de propósito único, con mínimo privilegio y credencial custodiada y rotada por la plataforma de accesos privilegiados; se prohíbe reutilizar credenciales humanas. El Adjudicatario entregará y mantendrá actualizado el inventario de todo flujo saliente de datos institucionales (origen, destino, tipo de dato, frecuencia y finalidad). La Convocante podrá suspender todo flujo no inventariado ni autorizado.

g) Nómina y cierre. El Adjudicatario mantendrá nómina nominada y actualizada del personal propio, subcontratado y del fabricante habilitado, con rol y alcance autorizado; las altas se comunicarán con cinco (5) días hábiles de anticipación y las bajas dentro de las veinticuatro (24) horas, plazo en el que se revocarán los accesos correspondientes. Concluida toda intervención que haya implicado conocimiento de credenciales, se procederá a su cambio dentro de los dos (2) días hábiles. Dentro de los cinco (5) días hábiles posteriores a la Recepción Técnica Definitiva y al término de la garantía se revocará la totalidad de los accesos, dejando constancia en acta. El Adjudicatario devolverá o destruirá de forma certificada toda copia de configuraciones, diagramas, inventarios, registros y credenciales del MTESS, incluidas las alojadas en su propia infraestructura, dentro de los treinta (30) días corridos de finalizado el contrato. El personal habilitado suscribirá acuerdo de confidencialidad individual con vigencia de cinco (5) años posteriores a la finalización del contrato.

h) Auditoría e incumplimiento. El Adjudicatario presentará informe mensual de accesos remotos dentro de los cinco (5) días hábiles del mes siguiente, y facilitará la evidencia que la Convocante requiera dentro de los tres (3) días hábiles. Constituyen incumplimiento contractual, con independencia de la producción de daño: el acceso sin autorización vigente o fuera de ventana; el uso de canales, herramientas o cuentas prohibidos; la omisión de notificar bajas en plazo; la alteración o eliminación de registros de sesión; y el establecimiento de flujos salientes no autorizados. Habilitan las penalidades del Contrato y del Pliego y, según su gravedad, la suspensión inmediata de todos los accesos remotos, sin eximir al Adjudicatario del cumplimiento de los tiempos del Acuerdo de Nivel de Servicio mediante asistencia presencial.

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:

Fecha(s) final(es) de entrega de los bienes: El proveedor dispondrá de 150 (ciento cincuenta) como máximo días calendario a partir del día siguiente de la fecha de emisión de la Orden de Compra para la entrega de los bienes y finalización de la instalación y puesta en funcionamiento, contados desde el día hábil siguiente a la recepción de la orden de ejecución.

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.

Fecha(s) final(es) de entrega de los servicios: El proveedor dispondrá de 150 (ciento cincuenta) como máximo días calendario a partir del día siguiente de la fecha de emisión de la Orden de Compra para la entrega de los bienes y finalización de la instalación y puesta en funcionamiento, contados desde el día hábil siguiente a la recepción de la orden de ejecución.

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 contractuales 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 ADMINISTRATIVOS” 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:

desde la suscripción del contrato hasta 90 días corridos posteriores al plazo de ejecución o vigencia del contrato, según sea el caso.

Si la entrega de los bienes o la prestación de los servicios, se realizare en un plazo menor o igual a diez (10) días 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 cláusula 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 <i>(se indica la fecha que debe presentar según el PBC)</i>
<i>Informe de avance</i>	Informe	Cada dos meses, desde la emisión de la primera orden de ejecución.

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 N° 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:

NOTA DE SOLICITUD DE PAGO CONTENIENDO LOS SIGUIENTES DATOS: NÚMERO DE RESOLUCIÓN QUE LO ADJUDICA COMO PROVEEDOR DE LOS SERVICIOS, NÚMERO DE CONTRATO Y LA DENOMINACIÓN ESPECÍFICA DEL PROCESO DE LICITACIÓN INDICADO EN EL SICP. DEBERA AGREGAR LA/S CONSTANCIA/S DE NO RETENCION DE IMPUESTO/S EN CASO DE NO SER SUJETO ALCANZADO SEGÚN NORMATIVA TRIBUTARIA, CASO CONTRARIO, SE APLICARAN TODAS LAS RETENCIONES ESTABLECIDAS EN LA LEGISLACION TRIBUTARIA.

LOS PAGOS DE LOS SIGUIENTES EJERCICIOS SE ENCUENTRAN SUJETOS A LA APROBACION CORRESPONDIENTE.

Plan de pagos

Concepto de pago	Porcentaje	Condición para el desembolso
Recepción de bienes materiales y equipos	30%	El pago se realizará contra la entrega completa, en el sitio designado por la Convocante, y previa verificación de todos los materiales y equipos previstos para la ejecución del proyecto, incluyendo firewalls, switches, puntos de acceso (AP) y los materiales del cableado correspondiente. Para autorizar el desembolso, será obligatoria la presentación del Acta de Recepción de Materiales y Equipos, debidamente suscrita por el equipo técnico designado por la Convocante. Esta recepción tendrá carácter provisorio y no implicará la aceptación definitiva de los bienes ni de la solución.
Primera Etapa de Instalación	30%	Comprenderá la instalación, terminación, identificación y certificación de 150 puntos de red, así como la sustitución de los racks seccionales, la interconexión de los switches mediante fibra óptica y la organización y el etiquetado integral de la infraestructura instalada. El desembolso estará sujeto a la presentación y aprobación de los resultados digitales de certificación de los enlaces instalados y del Acta de Avance Parcial, debidamente suscrita por el equipo técnico designado por la Convocante.
Segunda Etapa de Instalación	30%	Contra la conclusión integral de los trabajos, que comprenderá la desinstalación del cableado existente, la ejecución satisfactoria de las pruebas funcionales y la entrega de los planos, diagramas, inventarios e informes de certificación correspondientes. El desembolso estará sujeto a la presentación y aprobación de dicha documentación, así como a la suscripción del Acta de Recepción Técnica Provisoria por parte del equipo técnico designado por la Convocante.
Pago final	10%	El porcentaje restante será abonado una vez subsanadas todas las observaciones formuladas durante la recepción provisorio, entregada la documentación final debidamente actualizada y concluida la capacitación y transferencia de conocimientos. Para la gestión del pago, el Oferente deberá presentar la factura correspondiente al porcentaje pendiente, acompañada del Acta de Recepción Técnica Definitiva, debidamente suscrita por la Convocante, y a su vez de la carta compromiso en carácter de declaración jurada que acredite la disponibilidad de un banco de 150 horas de acompañamiento técnico, utilizable a requerimiento de la institución durante la vigencia de la garantía de 36 meses.

Condiciones generales de aplicación

Documentación de respaldo. Cada solicitud de pago deberá acompañarse de la factura legal correspondiente, el acta aplicable al hito, los informes técnicos y cualquier otro documento exigido por el contrato o por la normativa administrativa vigente.

Conformidad técnica. La emisión de las actas estará sujeta a la comprobación de cantidades, calidad, funcionamiento, etiquetado, certificación y cumplimiento de las especificaciones técnicas. La convocante podrá formular observaciones antes de otorgar la conformidad.

Pagos parciales. Los pagos parciales acreditan únicamente el avance certificado y no liberan al proveedor de su responsabilidad por defectos, incumplimientos, garantías o trabajos pendientes.

Variación de cantidades. Cualquier modificación de cantidades, alcance o distribución deberá contar con autorización previa y formal de la convocante y se tramitará conforme a las condiciones contractuales aplicables.

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 del Contrato estará sujeto a reajustes siempre y cuando el IPC, publicado por el BCP, haya sufrido una variación igual o mayor al 15% (quince por ciento) del vigente a la fecha de apertura de ofertas, conforme a la siguiente formula: $A = P \times I.I.B.C.P.$ A= Precio ajustado de los bienes y/o servicios conexos facturados. P= Precio facturados de los bienes y/o servicios conexos ofertados. I.I.B.C.P= Índice de Inflación emitido por el Banco Central del Paraguay. El reajuste solo será aplicado a solicitud del proveedor, el cual deberá hacerlo por escrito al administrador del contrato, y se dará curso si la contratante considere la correspondencia de la solicitud y dispone de suficiente disponibilidad presupuestaria. La solicitud debe realizarse indefectiblemente dentro del mes siguiente al cual se produjeron las variaciones, bajo pena de no poder solicitarlo posteriormente; y será aplicado únicamente sobre el saldo contractual no ejecutado o sobre los servicios pendientes a ser realizados, posteriores al mes en el cual se produjeron las variaciones. No se reconocerá reajuste de precios si el servicio se encuentra atrasado respecto al plan de entregas aprobado.

La variación del valor del contrato por reajuste de precios, no constituye modificación del contrato en los términos de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas", sin embargo, deberá contar con un Código de Contratación, 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:

1,00 %

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

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

Tasa de interés por Mora

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

0,01

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:

El proveedor o consultor o contratista realizará la solicitud de cobro dentro de los 5 (cinco) días hábiles posteriores al cobro del monto de la factura que incurriera en mora. Se deberá ingresar una nota dirigida al Administrador de Contrato

adjuntando los datos principales de la factura (número, fecha de emisión, monto y los datos de este proceso vinculado a la misma), comprobante de transferencia bancaria o cheque que acredite la fecha de recepción de los fondos y la planilla de liquidación, la cual consta de la siguiente fórmula:

$I = \text{Monto neto de la factura} \times \text{Tasa de interés diaria} \times \text{Días de atraso}$

El Administrador de Contratos emitirá un dictamen fundado dentro de los 10 (diez) días de recepción del pedido de cobro de mora, en la cual dictaminará si la falta de pago de la factura no sea imputable al contratista por falta de presentación de documentos u otros casos y si corresponde el monto aplicado en base a la fórmula mencionada. El Administrador de Contrato remitirá a la DGAF donde se gestionará la Disponibilidad Presupuestaria, así como el acto administrativo de la Máxima Autoridad Institucional donde se autorice el pago y la gestión del Código de Contratación especial.

Si el pago de la factura no se ha realizado, el Contratista podrá ejercer su derecho de suspensión del contrato (a partir de los 60 días) y presentará una solicitud de intereses devengados hasta esa fecha, sin perjuicio de la actualización posterior al momento del pago efectivo.

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

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 artículo 72 y concordantes de la Ley N° 7021/22.

Otras causales de terminación del contrato

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

No Aplica

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.

