

PLIEGO DE BASES Y CONDICIONES

Convocante:

**Ministerio de Desarrollo Social (MDS)
UOC SAS**

Nombre de la Licitación:

ADQUISICIÓN DE LICENCIAS DE SOFTWARE Y HARDWARE
(versión 4)

ID de Licitación:

401418



Modalidad:

Concurso de Ofertas

Publicado el:

29/09/2021

"Pliego para la Adquisición de Bienes y/o Servicios - Convencional"
Versión 1

RESUMEN DEL LLAMADO

Datos de la Convocatoria

| | | | |
|-------------------------|---------------------------------------|--------------------------|---|
| ID de Licitación: | 401418 | Nombre de la Licitación: | Adquisición de Licencias de Software y Hardware |
| Convocante: | Ministerio de Desarrollo Social (MDS) | Categoría: | 24 - Equipos, accesorios y programas computacionales, de oficina, educativos, de imprenta, de comunicación y señalamiento |
| Unidad de Contratación: | UOC SAS | Tipo de Procedimiento: | CO - Concurso de Ofertas |

Etapas y Plazos

| | | | |
|--------------------------------|---|-------------------------------|------------------|
| Lugar para Realizar Consultas: | Ciudad de Fndo. de la Mora. Avda. Mcal Lopez casi Cnel Pampliega- Edificio MDS 2do piso | Fecha Límite de Consultas: | 16/09/2021 09:00 |
| Lugar de Entrega de Ofertas: | Ciudad de Fndo. de la Mora. Avda. Mcal Lopez casi Cnel Pampliega- Edificio MDS 2do piso | Fecha de Entrega de Ofertas: | 05/10/2021 09:00 |
| Lugar de Apertura de Ofertas: | Ciudad de Fndo. de la Mora. Avda. Mcal Lopez casi Cnel Pampliega- Edificio MDS 2do piso | Fecha de Apertura de Ofertas: | 05/10/2021 09:30 |

Adjudicación y Contrato

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

Datos del Contacto

| | | | |
|-----------|------------------------------|---------------------|-----------------|
| Nombre: | Luis Rolando Portillo Romero | Cargo: | Director _ DUOC |
| Teléfono: | 021 678 458 | Correo Electrónico: | uoc@mds.gov.py |

ADENDA

Adenda

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

28/09/2021.

ADENDA 3.

La DUOC del Ministerio de Desarrollo Social emite la presente Adenda 3 al llamado a Concurso de Ofertas para "Adquisición de Licencias de Software y Hardware", ID. 401.418 de la DNCP, quedando redactado de la siguiente manera:

En el Sistema de Información de las Contrataciones Públicas (SICP) en Etapas y Plazos se ha modificado Fecha y Hora de Entrega de Ofertas; Fecha y Hora Apertura de Ofertas.

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

DATOS DE LA LICITACIÓN

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

Contratación Pública Sostenibles - CPS

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

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

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

Criterios sociales y económicos:

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

Criterios ambientales:

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

Conducta empresarial responsable:

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

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

Difusión de los documentos de la licitación

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

Aclaración de los documentos de la licitación

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

La convocante responderá por escrito a toda solicitud de aclaración del pliego de bases y condiciones que reciba dentro del plazo establecido o que se

derive de la Junta de Aclaraciones.

La convocante publicará una copia de su respuesta, incluida una explicación de la consulta, pero sin identificar su procedencia, a través del Sistema de Información de Contrataciones Públicas (SICP), dentro del plazo tope.

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

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

Documentos de la oferta

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

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

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

Oferentes en consorcio

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

Para ello deberán presentar escritura pública de constitución del consorcio o un acuerdo con el compromiso de formalizar el consorcio por escritura pública en caso de resultar adjudicados, antes de la firma del contrato.

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

Aclaración de las ofertas

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

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

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

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

Disconformidad, errores y omisiones

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

A tal efecto, el Comité de Evaluación emplazará por escrito al oferente a que presente la información o documentación necesaria, dentro de un plazo razonable establecido por el mismo, bajo apercibimiento de rechazo de la oferta. El Comité de Evaluación, podrá reiterar el pedido cuando la respuesta no resulte satisfactoria, toda vez que no 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 la oferente para su aceptación:

1. Si hay una discrepancia entre un precio unitario y el precio total obtenido al multiplicar ese precio unitario por las cantidades correspondientes, prevalecerá el precio unitario y el precio total será corregido.
2. Si hay un error en un total que corresponde a la suma o resta de subtotales, los subtotales prevalecerán y se corregirá el total
3. En caso de que el oferente haya cotizado su precio en guaraníes con décimos y céntimos, la convocante procederá a realizar el redondeo hacia abajo.
4. Si hay una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras a menos que la cantidad expresada en palabras corresponda a un error aritmético, en cuyo caso prevalecerán las cantidades en cifras de conformidad con los párrafos (1) y (2) mencionados.

Idioma de la oferta

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

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

No Aplica

Idioma del contrato

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

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

Moneda de la oferta y pago

La moneda de la oferta y pago será:

En Guaraníes para todos los oferentes

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

Visita al sitio de ejecución del contrato

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

No Aplica

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

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

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

Precio y formulario de la oferta

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

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

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

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

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

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

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

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

Abastecimiento simultáneo

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

No Aplica

Incoterms

La edición de incoterms para esta licitación será:

No Aplica

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

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

Autorización del Fabricante

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

Se solicita autorización del Fabricante para el Lote 1 Hardware de Red y para el Lote 2 Software Antivirus.

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

Muestras

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

No Aplica

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

Ofertas Alternativas

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

No Aplica

Copias de la oferta - CPS

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

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

Cantidad de copias requeridas:

0 copias

Formato y firma de la oferta

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

Periodo de validez de las ofertas

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

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

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

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

Garantías: instrumentación, plazos y ejecución.

1. La garantía de mantenimiento de oferta deberá expedirse en un monto en guaraníes que no deberá ser inferior al porcentaje especificado en el SICP. El oferente puede adoptar cualquiera de las formas de instrumentación de las garantías dispuestas por las normativas vigentes.
2. En los contratos abiertos, el porcentaje de las garantías a ser presentado por los oferentes que participen, deberá ser aplicado sobre el monto máximo del llamado; si la adjudicación fuese por lote o ítem ofertado, deberán sumarse los valores máximos de cada lote o ítem ofertado, a fin de obtener el monto sobre el cual se aplicará el porcentaje de la citada garantía.
3. En caso de instrumentarse a través de Garantía Bancaria, deberá estar sustancialmente de acuerdo con el formulario de Garantía de Mantenimiento de oferta incluido en la Sección "Formularios".
4. La garantía de mantenimiento de oferta en caso de oferentes en consorcio deberá ser presentado de la siguiente manera:
 - Consorcio constituido por escritura pública: deberán emitir a nombre del consorcio legalmente constituido por escritura pública, del líder del consorcio o de todos los socios que la integran;
 - Consorcio en proceso de formación con acuerdo de intención: deberán emitir a nombre del líder del consorcio en proceso de formación con acuerdo de intención o de todos los miembros que la integran.
5. La garantía de mantenimiento de ofertas podrá ser ejecutada:
 - a) Si el oferente altera las condiciones de su oferta,
 - b) Si el oferente retira su oferta durante el período de validez de la oferta,
 - c) Si no acepta la corrección aritmética del precio de su oferta, en caso de existir,
 - d) Si el adjudicatario no procede, por causa imputable al mismo a:
 - d.1. Suministrar los documentos indicados en el pliego de bases y condiciones para la firma del contrato,
 - d.2. Firmar el contrato,
 - d.3. Suministrar en tiempo y forma la garantía de cumplimiento de contrato,
 - d.4. Cuando se compruebe que las declaraciones juradas presentadas por el oferente adjudicado con su oferta sean falsas,
 - d.5. Si el adjudicatario no presentare las legalizaciones correspondientes para la firma del contrato, cuando éstas sean requeridas, o
 - d.6. No se formaliza el consorcio por escritura pública, antes de la firma del contrato.
6. Las garantías tanto de Mantenimiento de Oferta, Cumplimiento de Contrato o de Anticipo, sea cual fuere la forma de instrumentación adoptada, deberá ser pagadera ante solicitud escrita de la convocante donde se haga constar el monto reclamado, cuando se tenga acreditada una de las causales de ejecución de la póliza. En estos casos será requisito que previamente el oferente sea notificado del incumplimiento y la intimación de que se hará efectiva la ejecución del monto asegurado.
7. Si la entrega de los bienes o la prestación de los servicios se realizare en un plazo menor o igual a diez (10) días calendario, posteriores a la firma del contrato, la garantía de fiel cumplimiento deberá ser entregada antes del cumplimiento de la prestación.
8. La garantía de Fiel Cumplimiento de Contrato será liberada y devuelta al proveedor, a requerimiento de parte, a más tardar treinta (30) días contados a partir de la fecha de cumplimiento de las obligaciones del proveedor en virtud de contrato, incluyendo cualquier obligación relativa a la garantía de los bienes.

Periodo de Validez de la Garantía de Mantenimiento de Oferta

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

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

Porcentaje de Garantía de Fiel Cumplimiento de Contrato

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

10,00 %

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

Periodo de validez de la Garantía de Cumplimiento de Contrato

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

30 días posteriores al plazo de ejecución o vigencia del contrato.

Periodo de validez de la Garantía de los bienes

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

No Aplica

Tiempo de funcionamiento de los bienes

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

No Aplica

Plazo de reposición de bienes

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

2 (dos) días hábiles posteriores a la comunicación escrita al proveedor, por parte del Ministerio de Desarrollo Social.

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.

Cobertura de Seguro de los bienes

La cobertura de seguro requerida a los bienes será:

No Aplica

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

Sistema de presentación de ofertas

El Sistema de presentación de ofertas para esta licitación será:

Un sobre

Los sobres deberán:

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

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

Plazo para presentar las ofertas

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

La Convocante podrá a su discreción, extender el plazo originalmente establecido para la presentación de ofertas mediante una adenda. En este caso todos los derechos y obligaciones de la convocante y de los oferentes previamente sujetos a la fecha límite original para presentar las ofertas quedarán sujetos a la nueva fecha prorrogada.

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

Retiro, sustitución y modificación de las ofertas

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

2. Todas las comunicaciones deberán ser:

- a) Presentadas conforme a la forma de presentación e identificación de las ofertas y además los respectivos sobres deberán estar marcados "RETIRO",

"SUSTITUCION" o "MODIFICACION";

b) Recibidas por la convocante antes del plazo límite establecido para la presentación de las ofertas;

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

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

Apertura de ofertas

1. La Convocante abrirá las ofertas y en caso de que hubiere notificaciones de retiro, sustitución y modificación de ofertas presentadas, las leerá en el acto público con la presencia de los oferentes o sus representantes a la hora, en la fecha y el lugar establecidos en el SICP.

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

3. Primero se procederá a verificar de entre las ofertas recibidas por courier o entregadas personalmente, los sobres marcados como:

a) "RETIRO". Se leerán en voz alta y el sobre con la oferta correspondiente no será abierto sino devuelto al Oferente remitente. No se permitirá el retiro de ninguna oferta a menos que la comunicación de retiro pertinente contenga la autorización válida para solicitar el retiro y sea leída en voz alta en el acto de apertura de las ofertas.

b) "SUSTITUCION" se leerán en voz alta y se intercambiará con la oferta correspondiente que está siendo sustituida; la oferta sustituida no se abrirá y se devolverá al Oferente remitente. No se permitirá ninguna sustitución a menos que la comunicación de sustitución correspondiente contenga una autorización válida para solicitar la sustitución y sea leída en voz alta en el acto de apertura de las ofertas.

c) "MODIFICACION" se abrirán y leerán en voz alta con la oferta correspondiente. No se permitirá ninguna modificación a las ofertas a menos que la comunicación de modificación correspondiente contenga la autorización válida para solicitar la modificación y sea leída en voz alta en el acto de apertura de las ofertas. Solamente se considerarán en la evaluación los sobres que se abren y leen en voz alta durante el Acto de Apertura de las Ofertas.

4. Los representantes de los oferentes que participen en la apertura de las ofertas deberán contar con autorización suficiente para suscribir el acta y los documentos que soliciten, bastando para ello la presentación de una autorización escrita del firmante de la oferta, esta autorización podrá ser incluida en el sobre oferta o ser portado por el representante.

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

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

7. La falta de firma en un documento sustancial, es considerada una omisión sustancial que no podrá ser subsanada en ninguna oportunidad una vez abiertas las ofertas.

8. En el sistema de un solo sobre el acta de apertura deberá ser comunicada al Sistema de Información de Contrataciones Públicas para su difusión, dentro de los dos (02) días hábiles de la realización del acto de apertura.

9. En el sistema de doble sobre, el acta de apertura técnica deberá ser comunicada al 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.

REQUISITOS DE CALIFICACIÓN Y CRITERIOS DE EVALUACIÓN

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

Condición de Participación

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

Requisitos de Calificación

Capacidad Legal

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

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

A los efectos de la verificación de la existencia de prohibiciones o limitaciones contenidas en los incisos a) y b), m) y n) del artículo 40 de la Ley N° 2051/03, modificado por Ley N° 6716/2021, el comité de evaluación realizará el siguiente análisis:

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

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

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

Análisis de precios ofertados

Durante la evaluación de ofertas, luego de haber realizado la corrección de errores aritméticos y de ordenar las ofertas presentadas de menor a mayor, el Comité de Evaluación procederá a solicitar a los oferentes una explicación detallada de la composición del precio ofertado de cada ítem, rubro o partida adjudicable, conforme a los siguientes parámetros:

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

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

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

Certificado de Producto y Empleo Nacional - CPS

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

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.

a) Consorcios:

a.1. Provisión de Bienes

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

a.2. Provisión de Servicios (se entenderá por el término servicio aquello que comprende a los servicios en general, las consultorías, obras públicas y servicios relacionados a obras públicas).

Todos los integrantes del consorcio deben contar con el CPEN.

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

Margen de preferencia local - CPS

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

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

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

Requisitos documentales para 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.]

2. Garantía de Mantenimiento de Oferta (*)

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

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

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

5. Constancia de presentación de la Declaración Jurada de bienes y rentas, activos y pasivos ante la Contraloría General de la República, para los sujetos obligados según los incisos a) y b) del numeral 2 del art. 1 de la Ley N° 6355/19. (**)

| |
|---|
| 6. Declaración Jurada de Declaración de Miembros, de conformidad con el formulario estándar Sección Formularios (**) |
| 7. Certificado de Cumplimiento Tributario. (**) |
| 8. Patente Comercial del municipio en donde esté asentado el establecimiento principal del oferente. (**) |
| 9. Documentos legales |
| 9.1. Oferentes Individuales. Personas Físicas. |
| <ul style="list-style-type: none"> Fotocopia simple de la Cédula de Identidad del firmante de la oferta. (*) |
| <ul style="list-style-type: none"> Constancia de inscripción en el Registro Único de Contribuyentes - RUC. (*) |
| <ul style="list-style-type: none"> 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. (*) |
| 9.2. Oferentes Individuales. Personas Jurídicas. |
| <ul style="list-style-type: none"> Fotocopia simple de los documentos que acrediten la existencia legal de la persona jurídica tales como la Escritura Pública de Constitución y protocolización de los Estatutos Sociales. Los estatutos deberán estar inscriptos en la Sección Personas Jurídicas de la Dirección de Registros Públicos. (*) |
| <ul style="list-style-type: none"> Constancia de inscripción en el Registro Único de Contribuyentes y fotocopia simple de los Documentos de Identidad de los representantes o apoderados de la sociedad. |
| <ul style="list-style-type: none"> Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al oferente. Estos documentos pueden consistir en: un poder suficiente otorgado por Escritura Pública (no es necesario que esté inscripto en el Registro de Poderes); o los documentos societarios que justifiquen la representación del firmante, tales como las actas de asamblea y de directorio en el caso de las sociedades anónimas. (*) |
| 9.3. Oferentes en Consorcio. |
| <p>1. Cada integrante del consorcio que sea una persona física domiciliada en la República del Paraguay deberá presentar los documentos requeridos para Oferentes Individuales especificados en el apartado Oferentes individuales. Personas Físicas. Cada integrante del consorcio que sea una persona jurídica domiciliada en Paraguay deberá presentar los documentos requeridos para Oferentes Individuales Personas Jurídicas. (*)</p> |
| <p>2. Original o fotocopia del consorcio constituido o del acuerdo de intención de constituir el consorcio por escritura pública en caso de resultar adjudicados y antes de la firma del contrato. Las formalidades de los acuerdos de intención y de los consorcios serán determinadas por la Dirección Nacional de Contrataciones Públicas (DNCP). (*)</p> |
| <p>3. Fotocopia simple de los documentos que acrediten las facultades de los firmantes del acuerdo de intención de consorciarse. Estos documentos pueden consistir en (*):</p> <ul style="list-style-type: none"> Un poder suficiente otorgado por escritura pública por cada miembro del consorcio (no es necesario que esté inscripto en el Registro de Poderes); o Los documentos societarios de cada miembro del consorcio, que justifiquen la representación del firmante, tales como actas de asamblea y de directorio en el caso de las sociedades anónimas. |

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

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

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

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

Capacidad Financiera

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

- a. Ratio de Liquidez: activo corriente / pasivo corriente Deberá ser igual o mayor que 1, en promedio de los Años 2019 y 2020.
 - b. Endeudamiento: pasivo total / activo total: No deberá ser mayor a 0,80 en promedio de los Años 2019 y 2020.
 - c. Rentabilidad: Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital, del promedio de los dos últimos años declarados Año 2019 y 2020, no deberá ser negativo.
- Nota Consorcios: Todos los integrantes del Consorcio deben cumplir con los requerimientos financieros establecidos.

Requisitos documentales para la evaluación de la capacidad financiera

- a. Balances de los años 2019 y 2020 firmados por el/los Propietario/os de la firma y un Profesional Contador

Experiencia requerida

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

Demostrar la experiencia en provisión de software y hardware con facturaciones de venta y/o recepciones finales por un monto equivalente al 50 % como mínimo del monto total ofertado en la presente licitación, de los: tres últimos años (2018; 2019 y 2020)

Requisitos documentales para la evaluación de la experiencia

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

Capacidad Técnica

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

LOTE 1

Contar como mínimo con 1 ingeniero certificado del producto.

Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar certificados de inscripción en IPS.

Contar como mínimo con 2 ingenieros con certificaciones ITIL para garantizar la buena asistencia en soporte técnico.

El proveedor deberá tener la Certificación ISO 9001 Sistema de Gestión de Calidad y la Certificación ISO 27001 Sistema de Gestión de Seguridad de la Información para garantizar el buen servicio y respaldo del soporte local.

El proveedor deberá contar con una plataforma y/o sistema de ticket para atención de casos de soporte técnico, a fin de garantizar la respuesta de manera profesional y organizada.

El proveedor local deberá contar con una plataforma de autoservicio de preguntas frecuentes, con por lo menos 50 plantillas de respuesta para esos casos, dicha plataforma deberá estar integrada con el sistema del ticket del proveedor.

LOTE 2

Contar como mínimo con 3 ingenieros certificados con las certificaciones avanzadas del producto.

Contar como mínimo con 2 técnicos con certificaciones de cifrado.

Contar con por lo menos 2 técnicos con certificaciones en protección de servidores de correo antispaam.

Contar con por lo menos 2 técnicos con certificaciones en Detecciones y Respuesta de Endpoints.

Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar certificados de inscripción en IPS.

Contar como mínimo con 3 ingenieros con certificaciones ITIL para garantizar la buena asistencia en soporte técnico.

El proveedor deberá ser Canal Platinum de la Marca ofertada, para garantizar el buen servicio y respaldo del soporte local, para ello deberá presentar el certificado que lo avale.

El proveedor deberá tener la Certificación ISO 9001 Sistema de Gestión de Calidad y la Certificación ISO 27001 Sistema de Gestión de Seguridad de la Información para garantizar el buen servicio y respaldo del soporte local.

El proveedor deberá contar con una plataforma y/o sistema de ticket para atención de casos de soporte técnico, a fin de garantizar la respuesta de manera profesional y organizada.

El proveedor local deberá contar con una plataforma de autoservicio de preguntas frecuentes, con por lo menos 50 plantillas de respuesta para esos casos, dicha plataforma deberá estar integrada con el sistema del ticket del proveedor

Requisito documental para evaluar la capacidad técnica

1. LOTE 1: Currículos y Certificados de estudios de los profesionales y técnicos ofrecidos
2. Declaración Jurada de Salarios de los últimos seis meses, que el empleador utilizó para el pago del seguro social, en caso de que la documentación no esté contenida en la oferta o en el Sistema de Información de Proveedores del Estado (SIPE)
3. Certificación ISO 9001 Sistema de Gestión de Calidad y la Certificación ISO 27001 Sistema de Gestión de Seguridad de la Información
4. Declaración Jurada en la cual manifiesta contar con plataforma y/o sistema de ticket para atención de casos de soporte técnico y de autoservicio de preguntas frecuentes y plantilla de respuesta

2. LOTE 2: Currículos y Certificados de estudios de los profesionales y técnicos ofrecidos.
3. Declaración Jurada de Salarios de los últimos seis meses, que el empleador utilizó para el pago del seguro social, en caso de que la documentación no esté contenida en la oferta o en el Sistema de Información de Proveedores del Estado (SIPE).
4. Certificado que avale que el proveedor es Canal Platinum de la marca ofertada.
5. Certificación ISO 9001 Sistema de Gestión de Calidad y la Certificación ISO 27001 Sistema de Gestión de Seguridad de la Información.
6. Declaración Jurada en la cual manifiesta contar con plataforma y/o sistema de ticket para atención de casos de soporte técnico y de autoservicio de preguntas frecuentes y plantilla de respuesta

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 llamado, 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.

Nota1: Conforme a lo previsto en el Decreto reglamentario de la Ley de Contrataciones los adjudicatarios de los contratos resultantes de los procesos licitatorios, deberán inscribirse en el Sistema de Información de Proveedores del Estado - SIPE, como requisito previo a la emisión del Código de Contratación respectivo, no siendo la inscripción una exigencia para participar en el proceso tradicional.

SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS

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

Suministros y Especificaciones técnicas

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

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

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

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

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

| | | | | | |
|--------------------------|--|------------------------|---|--------------------|----------|
| LOTE 1 | | | | | |
| LOTE 1 - HARDWARE DE RED | | | | | |
| Item | Descripción General Para Montar un Data Center | Descripción Especifica | Especificaciones Técnicas | Exigencias mínimas | Cantidad |
| | | | Requerimientos Mínimos | | |
| | | | Puertos | | |
| | | | 10 x 100Mb / 1Gb / 10GBASE-X SFP+ puertos Como Mínimo. | Exigido | |
| | | | 1 USB 2.0 port Como Mínimo. | Exigido | |
| | | | 1 x puerto de consola serie RJ-45 Como Mínimo. | Exigido | |
| | | | 1 puerto de administración fuera de banda 10 / 100Base-T Como Mínimo. | Exigido | |
| | | | Actuación | | |
| | | | Velocidad de línea 200 Gbps / 148.8 Mpps Capacidad de conmutación. Como mínimo. | Exigido | |
| | | | Alimentación | | |
| | | | Fuente de alimentación 100W, Como minimo | Exigido | |
| | | | Conector RPS para PSU redundante externa, Como minimo | Exigido | |
| | | | Peso | | |
| | | | 2,74 kg, Como minimo. | Opcional | |
| | | | Dimensiones | | |

| | |
|--|----------|
| 12in W / 10.3in D / 1.7in H (30.48cm / 26.2cm / 4.3cm), Como minimo. | Opcional |
| Disipación de calor mínima (BTU / HR) | |
| 60 BTU/hr, Como minimo. | Exigido |
| Consumo mínimo de energía (vatios) | |
| 18 W, Como minimo. | Exigido |
| Máxima * Disipación de calor (BTU / HR) | |
| 123 BTU/hr, Como minimo. | Exigido |
| Máximo * consumo de energía (vatios) | |
| 36 W, Como minimo. | Exigido |
| Rango de temperatura | |
| 0° C to 50° C, Como minimo. | Exigido |
| Presión de sonido del espectador (dBA) | |
| 28.2 dB(A) / 66.3 dB(A) | Opcional |
| Potencia de sonido declarada (BA) | |
| 3.8 dB(A) / 7.9 dB(A) | Opcional |
| Velocidad del ventilador | |
| Bajo / alto | Exigido |
| Número de ventiladores en Switch | |
| Flujo de aire de lado a lado: como minimo | Exigido |
| Características / Estándares y Protocolos | |
| CPU / memoria | |
| • Procesador reloj de 1 GHz. Como minimo. | Exigido |
| • 1GHz de DRAM. Como minimo. | Exigido |
| • Flash de 4Gb eMMC. Como minimo. | Exigido |
| • búfer MAC de 2 MB. Como minimo. | Exigido |
| Especificaciones de plataforma | |
| • Direcciones MAC máximas: 16,000 Como minimo. | Exigido |
| • VLAN: hasta 4092 Como minimo. | Exigido |
| • Grupos de acceso a enlaces (M-LAG) Como minimo. | Exigido |
| • ACL: Entrada 2048 / salida 512 reglas por lista Como minimo. | Exigido |
| • Clases de tráfico (colas): 8 Como minimo. | Exigido |
| Switching - Características principales de conmutación | |
| • IEEE 802.3ab 1000BASE-T | Exigido |
| • IEEE 802.3z 1000BASE-X | Exigido |
| • IEEE 802.3ae 10GBASE-X | Exigido |

| | |
|---|---------|
| • IEEE 802.3an 10GBASE-T | Exigido |
| • IEEE 802.3az Energy Efficient Ethernet | Exigido |
| • IEEE 802.3bz 2.5GBASE-T | Exigido |
| • IEEE 802.3bz 5GBASE-T | Exigido |
| • IEEE 802.3u, 100Base-FX | Exigido |
| • IEEE 802.3at 30W PoE+ | Exigido |
| • IEEE 802.3bt 4-Pair 60W PoE++ | Exigido |
| • GVRP: registro dinámico de VLAN | Exigido |
| • RFC 4541 - Consideraciones para los conmutadores de indagación del Protocolo de administración (IGMP) | Exigido |
| • ANSI / TIA-1057 - LLDP-Media Endpoint Discovery (MED) | Exigido |

Características avanzadas de la capa 2

| | |
|--|---------|
| • IEEE 802.1D STP - Sin bucles en una red con enlaces redundantes. | Exigido |
| • IEEE 802.1w RSTP - Árbol de expansión rápida | Exigido |
| • IEEE 802.1s MSTP - Tabla de mapeo de VLAN | Exigido |
| • Compatible con (PVST+) - Prevenir bucles de Capa 2 en un entorno de red conmutada. | Exigido |
| • IEEE 802.1Q - Múltiples redes con interconectadas con puentes | Exigido |
| • EMISTP | Exigido |
| • Autenticación, autorización y contabilidad (AAA) | Exigido |
| • Broadcast / Multicast / Recuperación de tormenta unicast desconocida | Exigido |
| • DHCP Snooping | Exigido |
| • IGMP Snooping Querier | Exigido |
| • Registro de VLAN de multidifusión (MVR) | Exigido |
| • Protocolo de descubrimiento estándar de la industria (interoperabilidad CDP) | Exigido |
| • API de clasificación IPv6 | Exigido |
| • Soporte de trama Jumbo Ethernet | Exigido |
| • Bloqueo de puerto MAC | Exigido |
| • puerto espejo | Exigido |
| • puertos protegidos | Exigido |
| • Filtrado MAC estático | Exigido |
| • VLAN de voz | Exigido |
| • VLAN no autenticada | Exigido |
| • Servidor interno de autenticación 802.1X | Exigido |
| • Modo de monitor 802.1x | Exigido |
| • Escala de cliente 802.1x | Exigido |

| | |
|---|---------|
| • Dependencia de enlace | Exigido |
| • Protección RA IPv6 (sin estado) | Exigido |
| • Protector de bucle STP | Exigido |
| • STP Root Guard | Exigido |
| • Enrutamiento de la Guardia BPDU | Exigido |
| • Enrutamiento estático y RIP IPv4 (hasta 64 rutas) | Exigido |
| • ECMP | Exigido |
| • Regulación ICMP | Exigido |
| • Interfaces de bucle invertido | Exigido |
| • Multinetting | Exigido |
| • ARP y ARP Proxy | Exigido |
| • VLAN y enrutamiento basado en puertos | Exigido |
| • UDP Relay / IP Helper | Exigido |
| • Basado en políticas | Exigido |

Enrutamiento

| | |
|--|---------|
| • Enrutamiento como OSPF-2 y BGP4 se autentican a través de MD5 | Exigido |
| • RFC 5798 Protocolo de redundancia de enrutador virtual (VRRP) Versión 3 para IPv4 e IPv6 | Exigido |
| • IOS 10589 OSI IS-IS Protocolo de enrutamiento intradominio (RFC 1142) | Exigido |
| • Detección de reenvío bidireccional | Exigido |
| • RFC 1027 Uso de ARP para implementar puertas de enlace de subred transparentes (Proxy ARP) | Exigido |
| • Protocolo de información de enrutamiento RFC 1058 (RIP) | Exigido |
| • Mensajes de descubrimiento de enrutador ICMP RFC 1256 | Exigido |
| • Requisitos RFC 1812 para enrutadores IP versión 4 | Exigido |
| • Autenticación RFC 2082 RIP-2 MD5 | Exigido |
| • Relé DHCP RFC 2131 | Exigido |
| • RFC 2453 RIP v2 | Exigido |
| • RFC 3021 Uso de prefijos de 31 bits en enlaces punto a punto IPv4 | Exigido |

Apilamiento avanzado

| | |
|---|---------|
| • Gestión de IP única de toda la pila. | Exigido |
| • Funcionalidad de pila cruzada, como LAG, instancias MSTP, VLAN, etc., que abarca unidades miembro de pila | Exigido |
| • Plano de control centralizado | Exigido |
| • Configuración y sincronización de firmware | Exigido |
| • Inicialización automática de la pila y adición / eliminación de unidades y conmutación por error maestra | Exigido |

| | |
|--|---------|
| • Cuatro unidades miembro soportadas en una pila, Como mínimo. | Exigido |
| • Características de servicio para monitorear y diagnosticar el estado de la unidad | Exigido |
| Calidad de servicio - Listas de control de acceso (ACL) | |
| • Permitir / denegar acciones para IP entrante y clasificación de tráfico de capa 2 en función de: | Exigido |
| • ACL basado en el tiempo | Exigido |
| • Dirección IP de origen / destino | Exigido |
| • Puerto de origen / destino TCP / UDP | Exigido |
| • Tipo de protocolo IP | Exigido |
| • Campo Tipo de servicio (ToS) o servicios diferenciados (DSCP) | Exigido |
| • Dirección MAC de origen / destino | Exigido |
| • EtherType | Exigido |
| • Prioridad de usuario IEEE 802.1p (etiqueta VLAN externa y / o interna) | Exigido |
| • ID de VLAN (etiqueta de VLAN externa y / o interna) | Exigido |
| • RFC 1858 - Consideraciones de seguridad para el filtrado de fragmentos de IP | Exigido |
| • Atributos opcionales de la regla ACL | Exigido |
| • Asignar flujo a una cola de Clase de servicio (CoS) específica | Exigido |
| • Redirigir los flujos de tráfico coincidentes | Exigido |
| Servicios diferenciados (DiffServ) | |
| • Clasifique el tráfico según los mismos criterios que las ACL y, opcionalmente: | Exigido |
| • Marque los campos de encabezado IP DSCP o Precedencia | Exigido |
| • Controle el flujo a una velocidad específica con soporte compatible con dos colores | Exigido |
| • RFC 2474 - Definición del campo de servicios diferenciados (campo DS) en los encabezados IPv4 e IPv6 | Exigido |
| • RFC 2475: una arquitectura para servicios diferenciados | Exigido |
| • RFC 2597: grupo de reenvío asegurado por comportamiento de salto (PHB) | Exigido |
| • RFC 2697 - Policía de tasa única | Exigido |
| • RFC 3246 - PHB de reenvío acelerado | Exigido |
| • RFC 3260 - Nueva terminología y aclaraciones para DiffServ | Exigido |
| Configuración de asignación de colas de clase de servicio (CoS) | |
| • Auto-VoIP: configuración automática de CoS para VoIP | Exigido |
| • Asignación de IP DSCP a cola | Exigido |
| • Modo de confianza de interfaz configurable (IEEE 802.1p, DSCP o no confiable) | Exigido |
| • Velocidad de configuración de salida de interfaz | Exigido |
| • Prioridad estricta versus programación ponderada por cola | Exigido |

1

DATA CENTER Y
SUS
ACCESORIOSSwitch TIPO 1
CORE**Instalaciones del sistema**

2

| | |
|---|---------|
| • Instalación de registro de eventos y errores. | Exigido |
| • Tiempo de ejecución y capacidad de descarga de configuración | Exigido |
| • utilidad PING | Exigido |
| • Transferencias FTP a través de IPv4 / IPv6 | Exigido |
| • TACACS + | Exigido |
| • sFlow | Exigido |
| • RFC 768 - UDP | Exigido |
| • RFC 783 - TFTP | Exigido |
| • RFC 791 - IP | Exigido |
| • RFC 792 - ICMP | Exigido |
| • RFC 793 - TCP | Exigido |
| • RFC 826 - ARP | Exigido |
| • RFC 894 - Transmisión de datagramas IP a través de redes Ethernet | Exigido |
| • RFC 896 - Control de congestión en redes IP / TCP | Exigido |
| • RFC 951 - BOOTP | Exigido |
| • RFC 1034 - Nombres de dominio - conceptos e instalaciones | Exigido |
| • RFC 1035 - Nombres de dominio - implementación y especificación | Exigido |
| • RFC 1321: algoritmo de resumen de mensajes | Exigido |
| • RFC 1534 - Interoperabilidad entre BOOTP y DHCP | Exigido |
| • RFC 2021 - Base de información de administración de monitoreo de red remota versión 2 | Exigido |
| • RFC 2030 - Protocolo simple de tiempo de red (SNTP) | Exigido |
| • RFC 2131 - relé DHCP | Exigido |
| • RFC 2132: opciones de DHCP y extensiones de proveedor BOOTP | Exigido |
| • RFC 2819 - Base de información de administración de monitoreo de red remota | Exigido |
| • RFC 2865 - Cliente RADIUS | Exigido |
| • RFC 2866 - Contabilidad RADIUS | Exigido |
| • RFC 2868 - Atributos RADIUS para soporte de protocolo de túnel | Exigido |
| • RFC 2869 - Extensiones RADIUS | Exigido |
| • RFC 3579: soporte RADIUS para EAP | Exigido |
| • RFC 3580: pautas de uso de IEEE 802.1X RADIUS | Exigido |
| • RFC 3164: el protocolo BSD syslog | Exigido |
| • RFC 3580 - Pautas de uso de RADIUS 802.1X | Exigido |
| • RFC 5176 - Servidor de autorización dinámico (solo procesamiento DisconnectRequest) | Exigido |

| | |
|---|---------|
| • RFC 5424 - La administración del protocolo Syslog | Exigido |
| • CLI estándar de la industria | Exigido |
| • gestión de IPv6 | Exigido |
| • gestión de contraseñas | Exigido |
| • Correo electrónico de alertas | Exigido |
| • Soporte de instalación automática para imágenes de firmware y archivos de configuración | Exigido |
| • SNMP v1, v2 y v3 | Exigido |
| • SSH 1.5 y 2.0 | Exigido |
| • RFC 4252: protocolo de autenticación SSH | Exigido |
| • RFC 4253: protocolo de capa de transporte SSH | Exigido |
| • RFC 4254: protocolo de conexión SSH | Exigido |
| • RFC 4251: arquitectura de protocolo SSH | Exigido |
| • RFC 4716: formato de archivo de clave pública SECSH | Exigido |
| • RFC 4419: intercambio de grupo Diffie-Hellman para el protocolo de capa de transporte SSH | Exigido |
| • SSL 3.0 y TLS 1.0 | Exigido |
| • RFC 2246: el protocolo TLS, versión 1.0 | Exigido |
| • RFC 2818: HTTP sobre TLS | Exigido |
| • RFC 3268: conjuntos de cifrado AES para la seguridad de la capa de transporte | Exigido |
| • Copia segura (SCP) | Exigido |
| • Telnet | Exigido |
| • Web | Exigido |
| • Java Plug-in 1.6.0_01 y Java Script 1.3 | Exigido |
| Funciones de gestión avanzada | |
| • CLI estándar de la industria con las siguientes características: | Exigido |
| • capacidad de secuencias de comandos | Exigido |
| • Comando completado | Exigido |
| • Ayuda sensible al contexto | Exigido |
| • Cifrado de contraseña de usuario opcional | Exigido |
| • Servidor Telnet multisesión | Exigido |
| • Analizador de puerto de conmutador remoto (RSPAN) | Exigido |
| • Gestión basada en la nube | Exigido |
| • Soporte de Management Center | Exigido |
| SNMP MIB | |
| • RFC 1157 SNMPv1 | Exigido |

| | |
|--|---------|
| • RFC 1650 MIB similar a Ethernet (actualización de RFC 1213 para SNMPv2) | Exigido |
| • RFC 1901 a - 1908 SNMPv2c, SMIv2 y MIB-II revisado | Exigido |
| • RFC 2576 Coexistencia entre SNMP versión 1, versión 2 y versión 3 del marco de gestión de red estándar de Internet | Exigido |
| • RFC 3410 - 3415 SNMPv3, seguridad, cifrado y autenticación basados en el usuario | Exigido |
| • RFC 3416 - Operaciones de protocolo para la versión 2 de SNMP | Exigido |
| • RFC 3826: el algoritmo de cifrado del estándar de cifrado avanzado (AES) en el modelo de seguridad basado en el usuario SNMP | Exigido |
| • Seguridad basada en el usuario SNMPv3, con cifrado / autenticación | Exigido |
| Condiciones de operación | |
| • Temperatura de Operación: -40° C to 70° C | Exigido |
| • Humedad relativa de funcionamiento: 10% a 95% (sin condensación) | Exigido |
| • Altitud de operación: capaz de operar de manera normal entre altitudes comprendidas desde 0 hasta 3000 mts sobre el nivel del mar. | Exigido |
| Empaque y Almacenamiento | |
| • Temperatura de almacenamiento: -40 ° C a 70 ° C | Exigido |
| • Humedad: 10% a 95% de humedad relativa, sin condensación. | Exigido |
| • Choque empaquetado (medio seno): 180 m / s ² (18 G), 6 ms, 600 choques. Como Mínimo. | Exigido |
| • Vibración empaquetada: 5 a 62 Hz a una velocidad de 5 mm / s, 62 a 500 Hz a 0.2 G. Como Mínimo. | Exigido |
| • Vibración aleatoria empaquetada: 5 a 20 Hz a 1.0 ASD con 3 dB / oct. de 20 a 200 Hz. Como Mínimo. | Exigido |
| • Altura de caída empaquetada: 14 gotas como mínimo en lados y esquinas a 42 pulgadas (caja <15 kg). Como Mínimo. | Exigido |
| Especificaciones ambientales | |
| • EN / ETSI 300 019-2-1 v2.1.2 - Almacenamiento de clase 1.2 | Exigido |
| • EN / ETSI 300 019-2-2 v2.1.2 - Clase 2.3 Transporte | Exigido |
| • EN / ETSI 300 019-2-3 v2.1.2 - Clase 3.1e Operacional | Exigido |
| • EN / ETSI 300 753 (1997-10) - Ruido acústico | Exigido |
| • Vibración aleatoria ASTM D3580 sin embalaje 1,5 G | Exigido |
| Cumplimiento ambiental | |
| • UE RoHS 2011/65 / UE | Exigido |
| • EU WEEE 2012/19 / EU | Exigido |
| • China RoHS SJ / T 11363-2006 | Exigido |
| Normativa y seguridad ITE norteamericana | |
| • UL 60950-1 2a edición A2: 2014, Dispositivo listado (EE. UU.) | Exigido |
| • CSA 22.2 No. 60950-1 2a edición 2014 (Canadá) | Exigido |

| | |
|---|---------|
| • Cumple con FCC 21CFR 1040.10 (seguridad láser de EE. UU.) | Exigido |
| • Carta de aprobación de CDRH (aprobación de la FDA de EE. UU.) | Exigido |
| ITE europeo | |
| • EN 60950-1: 2006 + A11: 2009 + A1: 2010 + A12: 2011 + A2: 2013 2ª ed. | Exigido |
| • EN 60825-1: 2007 / IEC 60825-1: 2007 Clase 1 (seguridad láser) | Exigido |
| • 2006/35 / Directiva de bajo voltaje de la UE | Exigido |
| ITE internacional | |
| • Informe y certificado CB según IEC 60950-1 2a ed. + Diferencias nacionales | Exigido |
| • AS / NZS 60950-1 (Australia / Nueva Zelanda) | Exigido |
| Estándares EMI / EMC EMC norteamericano para ITE | |
| • FCC CFR 47 parte 15 Clase A (EE. UU.) | Exigido |
| • ICES-003 Clase A (Canadá) | Exigido |
| Estándares europeos de EMC | |
| • EN 55032: 2015 Clase A | Exigido |
| • EN 55024: 2012 | Exigido |
| • EN 61000-3-2:2014 (armónicos) | Exigido |
| • EN 61000-3-3 2013 (parpadeo) | Exigido |
| • EN 300386 v1.6.1 (Telecomunicaciones EMC) | Exigido |
| • 2014/30 / Directiva EMC de la UE | Exigido |
| Certificaciones internacionales de EMC | |
| • CISPR 22:2006 Ed 5.2, Class A (Emisiones internacionales) | Exigido |
| • CISPR 24:A2:2003 Class A (Inmunidad internacional) | Exigido |
| • IEC 61000-4-2: 2008 / EN 61000-4-2: 2009 Descarga electrostática, contacto de 8 kV, aire de 15 kV, criterio A | Exigido |
| • IEC 61000-4-3: 2008 / EN 61000-4-3: 2006 + A1: 2008 Inmunidad radiada 10 V / m, Criterio A | Exigido |
| • IEC 61000-4-4: 2004 am1 ed.2./EN 61000-4-4: 2004 / A1: 2010 Ráfaga transitoria, 1 kV, Criterio A | Exigido |
| • IEC 61000-4-5: 2005 / EN 61000-4-5: 2006 Sobretensión, 2 kV L-L, 2 kV L-G, Nivel 3, Criterio A | Exigido |
| • IEC 61000-4-6: 2008 / EN 61000-4-6: 2009 Inmunidad conducida, 0,15-80 MHz, 10 V / m unmod. RMS, Criterio A | Exigido |
| • IEC / EN 61000-4-11: 2004 Caídas e interrupciones de energía,> 30%, 25 períodos, Criterio C | Exigido |
| País específico | |
| • VCCI Clase A (Emisiones de Japón) | Exigido |
| • ACMA RCM (Emisiones de Australia) | Exigido |
| • Marca CCC | Exigido |

| | |
|---|----------|
| • Marca KCC, Aprobación EMC (Corea) | Exigido |
| Certificacion | |
| • Ingeniero CERTIFICADO por la marca. | Exigido |
| • Tecnico CERTIFICADO por la marca. | Exigido |
| Terminos a Tener en Cuenta | |
| 1.1. Contar como mínimo con 1 ingeniero certificado del producto | |
| 1.2. Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar certificados de inscripción en IPS | |
| 1.3. contar como mínimo con 2 ingenieros con certificaciones ITIL para garantizar la buena asistencia en soporte técnico. | |
| 1.4. contar con 10 contratos o facturas de la provisión de Software y/o Hardware de seguridad ofertado entre los años 2018, 2019 y 2020. | |
| 1.5. Configuración de los equipos de acuerdo a las políticas de la entidad. | |
| 1.6. capacitación de todas las personas involucradas en el departamento de tecnología. | |
| 1.7. soporte técnico incluido local y del fabricante | |
| 1.8. cantidad de tickets de soporte ilimitados. | |
| 1.9. El proveedor deberá tener la Certificación ISO 9001 Sistema de Gestión de Calidad y la Certificación ISO 27001 Sistema de Gestión de Seguridad de la Información para garantizar el buen servicio y respaldo del soporte local. | Exigido |
| 1.10. El proveedor deberá presentar autorización del fabricante expresamente dirigido a la convocante refiriendo el nro. de ID del llamado | |
| 1.11. El proveedor deberá contar con una plataforma y/o sistema de ticket para atención de casos de soporte técnico, a fin de garantizar la respuesta de manera profesional y organizada. | |
| 1.12. El proveedor local deberá contar con una plataforma de autoservicio de preguntas frecuentes, con por lo menos 50 plantillas de respuesta para esos casos, dicha plataforma deberá estar integrada con el sistema del ticket del proveedor | |
| 1.13. la convocante podrá solicitar si cree necesario a los oferentes una demostración del manejo y despliegue de la herramienta | |
| Requerimientos Mínimos | |
| Puertos | |
| • 24 puertos 10/100/1000BaseT (RJ-45). Como Minimo. | Exigido |
| • 2 puertos 1GBASE-X (SFP) despoblados. Como Minimo. | Exigido |
| • 1 x puerto de consola serie RJ-45. Como Minimo. | Exigido |
| • 1 puerto de administración fuera de banda 10 / 100Base-T. Como Minimo. | Exigido |
| Actuación | |
| Velocidad de línea 52 Gbps / 38.7 Mpps Capacidad de conmutación. Como minimo. | Exigido |
| Alimentación | |
| Interna, RPS Opcional, Como minimo. | Exigido |
| Peso | |
| 3.13 kg, Como minimo. | Opcional |
| Dimensiones | |
| 4.4 cm (H) x 44.1 cm (W) x 25.4 cm (D) 1.73 (H) x 17.38 (W) x 10.0 (D), Como minimo. | Exigido |
| Disipación de calor mínima (BTU / HR) | |
| 56, Como minimo. | Exigido |
| Consumo mínimo de energía (vatios) | |
| | Exigido |

| | |
|---|---------|
| 16, Como minimo. | Exigido |
| Máxima * Disipación de calor (BTU / HR) | Exigido |
| 87, Como minimo. | Exigido |
| Máximo * consumo de energía (vatios) | Exigido |
| 26, Como minimo. | |
| Rango de temperatura | |
| 0C-40C / 40C-50C, Como minimo. | Exigido |
| Presión de sonido del espectador (dBA) | Exigido |
| 43,5 / 52,9, Como minimo. | Exigido |
| Potencia de sonido declarada (BA) | Exigido |
| 5.6 / 6.7, Como minimo. | Exigido |
| Velocidad del ventilador | |
| Bajo / alto, Como minimo. | Exigido |
| Número de ventiladores en Switch | |
| 2, Como minimo. | Exigido |
| Características / Estándares y Protocolos | |
| CPU / memoria | |
| • Procesador ARM Cortex-A9 32-bit, 400 MHz clock Como minimo. | Exigido |
| • 512 MB de DRAM Como minimo. | Exigido |
| • Flash de 128 MB Como minimo. | Exigido |
| • búfer MAC de 1,5 MB; 128K L2 Caché (CPU) Como minimo. | Exigido |
| Especificaciones de plataforma | |
| • Direcciones MAC máximas: 16,000. Como Minimo. | Exigido |
| • VLAN: hasta 1024 • Instancias MSTP: 4. Como Minimo. | Exigido |
| • Grupos de acceso a enlaces (LAG): 6. Como Minimo. | Exigido |
| • ACL: 100 con 1023 reglas por lista. Como Minimo. | Exigido |
| • Clases de tráfico (colas): 8. Como Minimo. | Exigido |
| Switching - Características principales de conmutación | |
| • IEEE 802.1ab - Protocolo de descubrimiento de capa de enlace (LLDP) | Exigido |
| • IEEE 802.1d: compatibilidad con árboles de expansión | Exigido |
| • IEEE 802.1p: prioridad de Ethernet con aprovisionamiento y mapeo de usuarios | Exigido |
| • IEEE 802.1s: compatibilidad con múltiples árboles de expansión | Exigido |
| • IEEE 802.1q: LAN virtuales con VLAN basadas en puertos | Exigido |
| • IEEE 802.1x: autenticación basada en puertos con compatibilidad con VLAN invitada | Exigido |
| • IEEE 802.1w: compatibilidad rápida de árbol de expansión | Exigido |

| | |
|---|---------|
| • IEEE 802.3 - 10BASE-T | Exigido |
| • IEEE 802.3u - 100BASE-T | Exigido |
| • IEEE 802.3ab - 1000BASE-T | Exigido |
| • IEEE 802.1ak: redes de área local con puente virtual | Exigido |
| • IEEE 802.3ac: etiquetado de VLAN | Exigido |
| • IEEE 802.3ad: agregación de enlaces | Exigido |
| • IEEE 802.3az: Ethernet de eficiencia energética en puertos 10/100/1000 | Exigido |
| • IEEE 802.3x - Control de flujo | Exigido |
| • GARP - Protocolo de registro de atributos genéricos | Exigido |
| • GMRP: registro multidifusión dinámico L2 | Exigido |
| • GVRP: registro dinámico de VLAN | Exigido |
| • RFC 4541 - Consideraciones para los conmutadores de indagación del Protocolo de administración (IGMP) | Exigido |
| • ANSI / TIA-1057 - LLDP-Media Endpoint Discovery (MED) | Exigido |
| • RFC 5171 - Protocolo de detección de enlace unidireccional (UDLD) | Exigido |

Características avanzadas de la capa 2

| | |
|--|---------|
| • Autenticación, autorización y contabilidad (AAA) | Exigido |
| • Broadcast / Multicast / Recuperación de tormenta unicast desconocida | Exigido |
| • DHCP Snooping | Exigido |
| • IGMP Snooping Querier | Exigido |
| • Registro de VLAN de multidifusión (MVR) | Exigido |
| • Protocolo de descubrimiento estándar de la industria (interoperabilidad CDP) | Exigido |
| • API de clasificación IPv6 | Exigido |
| • Soporte de trama Jumbo Ethernet | Exigido |
| • Bloqueo de puerto MAC | Exigido |
| • puerto espejo | Exigido |
| • puertos protegidos | Exigido |
| • Filtrado MAC estático | Exigido |
| • VLAN de voz | Exigido |
| • VLAN no autenticada | Exigido |
| • Servidor interno de autenticación 802.1X | Exigido |
| • Modo de monitor 802.1x | Exigido |
| • Escala de cliente 802.1x | Exigido |
| • Dependencia de enlace | Exigido |
| • Protección RA IPv6 (sin estado) | Exigido |
| • Protector de bucle STP | Exigido |

| | |
|---|---------|
| • STP Root Guard | Exigido |
| • Enrutamiento de la Guardia BPDU | Exigido |
| • Enrutamiento estático y RIP IPv4 (hasta 64 rutas) | Exigido |
| • ECMP | Exigido |
| • Regulación ICMP | Exigido |
| • Interfaces de bucle invertido | Exigido |
| • Multinetting | Exigido |
| • ARP y ARP Proxy | Exigido |
| • VLAN y enrutamiento basado en puertos | Exigido |
| • UDP Relay / IP Helper | Exigido |
| • Basado en políticas | Exigido |
| Enrutamiento | |
| • Enrutamiento estático de capa 3 con 60 rutas para la segmentación de la red | Exigido |
| • Proporciona enrutamiento básico a través de la configuración de enrutamiento manual | Exigido |
| Apilamiento avanzado | |
| • Gestión de IP única de toda la pila. | Exigido |
| • Funcionalidad de pila cruzada, como LAG, instancias MSTP, VLAN, etc., que abarca unidades miembro de pila | Exigido |
| • Plano de control centralizado | Exigido |
| • Configuración y sincronización de firmware | Exigido |
| • Inicialización automática de la pila y adición / eliminación de unidades y conmutación por error maestra | Exigido |
| • Cuatro unidades miembro soportadas en una pila | Exigido |
| • Características de servicio para monitorear y diagnosticar el estado de la unidad | Exigido |
| Calidad de servicio - Listas de control de acceso (ACL) | |
| • Permitir / denegar acciones para IP entrante y clasificación de tráfico de capa 2 en función de: | Exigido |
| • ACL basado en el tiempo | Exigido |
| • Dirección IP de origen / destino | Exigido |
| • Puerto de origen / destino TCP / UDP | Exigido |
| • Tipo de protocolo IP | Exigido |
| • Campo Tipo de servicio (ToS) o servicios diferenciados (DSCP) | Exigido |
| • Dirección MAC de origen / destino | Exigido |
| • EtherType | Exigido |
| • Prioridad de usuario IEEE 802.1p (etiqueta VLAN externa y / o interna) | Exigido |
| • ID de VLAN (etiqueta de VLAN externa y / o interna) | Exigido |

| | |
|--|---------|
| • RFC 1858 - Consideraciones de seguridad para el filtrado de fragmentos de IP | Exigido |
| Atributos opcionales de la regla ACL | Exigido |
| • Asignar flujo a una cola de Clase de servicio (CoS) específica | Exigido |
| • Redirigir los flujos de tráfico coincidentes | Exigido |
| Servicios diferenciados (DiffServ) | |
| • Clasifique el tráfico según los mismos criterios que las ACL y, opcionalmente: | Exigido |
| • Marque los campos de encabezado IP DSCP o Precedencia | Exigido |
| • Controle el flujo a una velocidad específica con soporte compatible con dos colores | Exigido |
| • RFC 2474 - Definición del campo de servicios diferenciados (campo DS) en los encabezados IPv4 e IPv6 | Exigido |
| • RFC 2475: una arquitectura para servicios diferenciados | Exigido |
| • RFC 2597: grupo de reenvío asegurado por comportamiento de salto (PHB) | Exigido |
| • RFC 2697 - Policía de tasa única | Exigido |
| • RFC 3246: un PHB de reenvío acelerado | Exigido |
| • RFC 3260 - Nueva terminología y aclaraciones para DiffServ | Exigido |
| Configuración de asignación de colas de clase de servicio (CoS) | |
| • Auto-VoIP: configuración automática de CoS para VoIP | Exigido |
| • Asignación de IP DSCP a cola | Exigido |
| • Modo de confianza de interfaz configurable (IEEE 802.1p, DSCP o no confiable) | Exigido |
| • Velocidad de configuración de salida de interfaz | Exigido |
| • Prioridad estricta versus programación ponderada por cola | Exigido |
| Instalaciones del sistema | |
| • Instalación de registro de eventos y errores. | Exigido |
| • Tiempo de ejecución y capacidad de descarga de configuración | Exigido |
| • utilidad PING | Exigido |
| • Xmodem | Exigido |
| • Transferencias FTP a través de IPv4 / IPv6 | Exigido |
| • Detección de código malicioso | Exigido |
| • TACACS + | Exigido |
| • sFlow | Exigido |
| • RFC 768 - UDP | Exigido |
| • RFC 783 - TFTP | Exigido |
| • RFC 791 - IP | Exigido |
| • RFC 792 - ICMP | Exigido |
| • RFC 793 - TCP | Exigido |

2

DATA CENTER Y
SUS
ACCESORIOSSwitch TIPO 2
DISTRIBUCION

| | |
|---|---------|
| • RFC 826 - ARP | Exigido |
| • RFC 894 - Transmisión de datagramas IP a través de redes Ethernet | Exigido |
| • RFC 896 - Control de congestión en redes IP / TCP | Exigido |
| • RFC 951 - BOOTP | Exigido |
| • RFC 1034 - Nombres de dominio - conceptos e instalaciones | Exigido |
| • RFC 1035 - Nombres de dominio - implementación y especificación | Exigido |
| • RFC 1321: algoritmo de resumen de mensajes | Exigido |
| • RFC 1534 - Interoperabilidad entre BOOTP y DHCP | Exigido |
| • RFC 2021 - Base de información de administración de monitoreo de red remota versión 2 | Exigido |
| • RFC 2030 - Protocolo simple de tiempo de red (SNTP) | Exigido |
| • RFC 2131 - relé DHCP | Exigido |
| • RFC 2132: opciones de DHCP y extensiones de proveedor BOOTP | Exigido |
| • RFC 2819 - Base de información de administración de monitoreo de red remota | Exigido |
| • RFC 2865 - Cliente RADIUS | Exigido |
| • RFC 2866 - Contabilidad RADIUS | Exigido |
| • RFC 2868 - Atributos RADIUS para soporte de protocolo de túnel | Exigido |
| • RFC 2869 - Extensiones RADIUS | Exigido |
| • RFC 3579: soporte RADIUS para EAP | Exigido |
| • RFC 3580: pautas de uso de IEEE 802.1X RADIUS | Exigido |
| • RFC 3164: el protocolo BSD syslog | Exigido |
| • RFC 3580 - Pautas de uso de RADIUS 802.1X | Exigido |
| • RFC 5176 - Servidor de autorización dinámico (solo procesamiento DisconnectRequest) | Exigido |
| • RFC 5424 - La administración del protocolo Syslog | Exigido |
| • CLI estándar de la industria | Exigido |
| • gestión de IPv6 | Exigido |
| • gestión de contraseñas | Exigido |
| • Correo electrónico de alertas | Exigido |
| • Soporte de instalación automática para imágenes de firmware y archivos de configuración | Exigido |
| • SNMP v1, v2 y v3 | Exigido |
| • SSH 1.5 y 2.0 | Exigido |
| • RFC 4252: protocolo de autenticación SSH | Exigido |
| • RFC 4253: protocolo de capa de transporte SSH | Exigido |
| • RFC 4254: protocolo de conexión SSH | Exigido |
| • RFC 4251: arquitectura de protocolo SSH | Exigido |

3

| | |
|---|---------|
| • RFC 4716: formato de archivo de clave pública SECSH | Exigido |
| • RFC 4419: intercambio de grupo Diffie-Hellman para el protocolo de capa de transporte SSH | Exigido |
| • SSL 3.0 y TLS 1.0 | Exigido |
| • RFC 2246: el protocolo TLS, versión 1.0 | Exigido |
| • RFC 2818: HTTP sobre TLS | Exigido |
| • RFC 3268: conjuntos de cifrado AES para la seguridad de la capa de transporte | Exigido |
| • Copia segura (SCP) | Exigido |
| • TACAS + | Exigido |
| • Telnet | Exigido |
| • Web | Exigido |
| • Java Plug-in 1.6.0_01 y Java Script 1.3 | Exigido |

Funciones de gestión avanzada

| | |
|--|---------|
| • CLI estándar de la industria con las siguientes características: | Exigido |
| • capacidad de secuencias de comandos | Exigido |
| • Comando completado | Exigido |
| • Ayuda sensible al contexto | Exigido |
| • Cifrado de contraseña de usuario opcional | Exigido |
| • Servidor Telnet multisesión | Exigido |
| • Analizador de puerto de conmutador remoto (RSPAN) | Exigido |
| • Gestión basada en la nube | Exigido |
| • Soporte Management Center | Exigido |

SNMP MIB

| | |
|--|---------|
| • MIB IEEE 802.1x (Revisión IEEE 802.1-PAEMIB 2004) | Exigido |
| • IEEE 802.3ad MIB (IEEE 802.3-ADMIB) | Exigido |
| • IANAifType-MIB | Exigido |
| • RFC 1213 - MIB II | Exigido |
| • RFC 1493 - Puente MIB | Exigido |
| • RFC 1612 - Extensiones MIB de resolución DNS | Exigido |
| • RFC 1643: definiciones de objetos administrados para los tipos de interfaz tipo Ethernet | Exigido |
| • RFC 2233: MIB de grupo de interfaces con SMI v2 | Exigido |
| • RFC 2613 - MIB SMON | Exigido |
| • RFC 2618 - MIB de cliente de autenticación RADIUS | Exigido |
| • RFC 2620 - MIB de contabilidad RADIUS | Exigido |
| • RFC 2674 - VLAN MIB | Exigido |

| | |
|--|---------|
| • RFC 2737 - Entidad MIB versión 2 | Exigido |
| • RFC 2819 - RMON grupos 1, 2, 3 y 9 | Exigido |
| • RFC 2863 - IF-MIB | Exigido |
| • RFC 2925: definiciones de objetos administrados para operaciones remotas de ping, tracer router y búsqueda | Exigido |
| • RFC 3273 - RMON MIB para redes de alta capacidad | Exigido |
| • RFC 3291 - Convenciones textuales para direcciones de red de Internet | Exigido |
| • RFC 3434 - Extensiones RMON MIB para alarmas de alta capacidad | Exigido |
| • RFC 4022 - TCP-MIB | Exigido |
| • RFC 4113 - UDP-MIB | Exigido |
| • RFC 2096: tabla de reenvío IP MIB | Exigido |
| • RFC 3636 - MIB MAU | Exigido |
| • RFC 3289 - Base de información de administración para la arquitectura DiffServ (solo lectura) | Exigido |

Condiciones de operación

| | |
|--|---------|
| • Temperatura de funcionamiento: 0°C a 50 ° C | Exigido |
| • Humedad relativa de funcionamiento: 10% a 95% (sin condensación) | Exigido |
| • Altitud de operación: capaz de operar de manera normal entre altitudes comprendidas desde 0 hasta 3000 mts sobre el nivel del mar. | Exigido |

Empaque y Almacenamiento

| | |
|---|---------|
| • Temperatura de almacenamiento: -40 ° C a 70 ° C (-40 ° F a 158 ° F) | Exigido |
| • Humedad: 10% a 95% de humedad relativa, sin condensación. | Exigido |
| • Choque empaquetado (medio seno): 180 m / s ² (18 G), 6 ms, 600 choques | Exigido |
| • Vibración empaquetada: 5 a 62 Hz a una velocidad de 5 mm / s, 62 a 500 Hz a 0.2 G | Exigido |
| • Vibración aleatoria empaquetada: 5 a 20 Hz a 1.0 ASD con 3 dB / oct. de 20 a 200 Hz | Exigido |
| • Altura de caída empaquetada: 14 gotas como mínimo en lados y esquinas a 42 pulgadas (caja <15 kg) | Exigido |

Especificaciones ambientales

| | |
|--|---------|
| • EN / ETSI 300 019-2-1 v2.1.2 - Almacenamiento de clase 1.2 | Exigido |
| • EN / ETSI 300 019-2-2 v2.1.2 - Clase 2.3 Transporte | Exigido |
| • EN / ETSI 300 019-2-3 v2.1.2 - Clase 3.1e Operacional | Exigido |
| • EN / ETSI 300 753 (1997-10) - Ruido acústico | Exigido |
| • Vibración aleatoria ASTM D3580 sin embalaje 1,5 G | Exigido |

Cumplimiento ambiental

| | |
|------------------------|---------|
| • UE RoHS 2011/65 / UE | Exigido |
| • EU WEEE 2012/19 / EU | Exigido |

| | |
|---|---------|
| • China RoHS SJ / T 11363-2006 | Exigido |
| Normativa y seguridad ITE norteamericana | |
| • UL 60950-1 2a edición A2: 2014, Dispositivo listado (EE. UU.) | Exigido |
| • CSA 22.2 No. 60950-1 2a edición 2014 (Canadá) | Exigido |
| • Cumple con FCC 21CFR 1040.10 (seguridad láser de EE. UU.) | Exigido |
| • Carta de aprobación de CDRH (aprobación de la FDA de EE. UU.) | Exigido |
| ITE europeo | |
| • EN 60950-1: 2006 + A11: 2009 + A1: 2010 + A12: 2011 + A2: 2013 2ª ed. | Exigido |
| • EN 60825-1: 2007 / IEC 60825-1: 2007 Clase 1 (seguridad láser) | Exigido |
| • 2014/35 / Directiva de bajo voltaje de la UE | Exigido |
| ITE internacional | |
| • Informe y certificado CB según IEC 60950-1: 2005 + A1: 2009 + A2: 2013 + Diferencias nacionales | Exigido |
| • AS / NZS 60950-1 (Australia / Nueva Zelanda) | Exigido |
| Estándares EMI / EMC EMC norteamericano para ITE | |
| • FCC CFR 47 parte 15 Clase A (EE. UU.) | Exigido |
| • ICES-003 Clase A (Canadá) | Exigido |
| Estándares europeos de EMC | |
| • EN 55032: 2015 Clase A | Exigido |
| • EN 55024: 2012 | Exigido |
| • EN 61000-3-2, 2014 (armónicos) | Exigido |
| • EN 61000-3-3 2013 (parpadeo) | Exigido |
| • EN 300386 v1.6.1 (Telecomunicaciones EMC) | Exigido |
| • 2014/30 / Directiva EMC de la UE | Exigido |
| Certificaciones internacionales de EMC | |
| • CISPR 32: 2015, Clase A (Emisiones internacionales) | Exigido |
| • AS / NZS CISPR32: 2013 | Exigido |
| • CISPR 24: 2010 Clase A (Inmunidad internacional) | Exigido |
| • IEC 61000-4-2: 2008 / EN 61000-4-2: 2009 Descarga electrostática, contacto de 8 kV, aire de 15 kV, Criterio A | Exigido |
| • IEC 61000-4-3: 2010 / EN 61000-4-3: 2006 + A1: 2008 + A2: 2010 Inmunidad radiada 10V / m, Criterio A | Exigido |
| • IEC 61000-4-4: 2012. / EN 61000-4-4: Explosión transitoria 2012, 1 kV, Criterio A | Exigido |
| • IEC 61000-4-5: 2014 / EN 61000-4-5: 2014 Sobretensión, 2 kV L-L, 2 kV L-G, Nivel 3, Criterios A | Exigido |
| • IEC 61000-4-6: 2013 / EN 61000-4-6: 2014 Inmunidad conducida, 0.15-80 MHz, 10V / m sin modificar. RMS. | Exigido |

| | |
|---|---------|
| • IEC / EN 61000-4-11: interrupciones e interrupciones de energía en 2004,> 30%, 25 períodos, Criterios C | Exigido |
|---|---------|

| | |
|------------------------|--|
| País específico | |
|------------------------|--|

| | |
|-------------------------------------|---------|
| • VCCI Clase A (Emisiones de Japón) | Exigido |
| • ACMA RCM (Emisiones de Australia) | Exigido |
| • Marca CCC | Exigido |
| • Marca KCC, Aprobación EMC (Corea) | Exigido |
| • Taiwán BSMI | Exigido |
| • Brasil Anatel | Exigido |
| • Rusia EAC | Exigido |

| | |
|---------------------------|--|
| Instalacion Switch | |
|---------------------------|--|

| | |
|---------------------------------------|---------|
| • Ingeniero CERTIFICADO por la marca. | Exigido |
| • Tecnico CERTIFICADO por la marca. | Exigido |

| | |
|-----------------------------------|--|
| Terminos a Tener en Cuenta | |
|-----------------------------------|--|

| | |
|---|---------|
| 1.1. Contar como mínimo con 1 ingeniero certificado del producto 1.2. Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar certificados de inscripción en IPS 1.3. contar como mínimo con 2 ingenieros con certificaciones ITIL para garantizar la buena asistencia en soporte técnico. 1.4. contar con 10 contratos o facturas de la provisión de Software y/o Hardware de seguridad ofertado entre los años 2018, 2019 y 2020. 1.5. Configuración de los equipos de acuerdo a las políticas de la entidad. 1.6. capacitación de todas las personas involucradas en el departamento de tecnología. 1.7. soporte técnico incluido local y del fabricante 1.8. cantidad de tickets de soporte ilimitados. 1.9. El proveedor deberá tener la Certificación ISO 9001 Sistema de Gestión de Calidad y la Certificación ISO 27001 Sistema de Gestión de Seguridad de la Información para garantizar el buen servicio y respaldo del soporte local. 1.10. El proveedor deberá presentar autorización del fabricante expresamente dirigido a la convocante refiriendo el nro. de ID del llamado 1.11. El proveedor deberá contar con una plataforma y/o sistema de ticket para atención de casos de soporte técnico, a fin de garantizar la respuesta de manera profesional y organizada. 1.12. El proveedor local deberá contar con una plataforma de autoservicio de preguntas frecuentes, con por lo menos 50 plantillas de respuesta para esos casos, dicha plataforma deberá estar integrada con el sistema del ticket del proveedor 1.13. la convocante podrá solicitar si cree necesario a los oferentes una demostración del manejo y despliegue de la herramienta | Exigido |
|---|---------|

| | |
|-------------------------------|--|
| Requerimientos Mínimos | |
|-------------------------------|--|

| | |
|-------------------|--|
| Compatible | |
|-------------------|--|

| | |
|-----------------------|---------|
| Marca y Modelo Switch | Exigido |
|-----------------------|---------|

| | |
|--------------------------|--|
| Redes compatibles | |
|--------------------------|--|

| | |
|---------------|---------|
| 10GB-F01-SFPP | Exigido |
|---------------|---------|

| | |
|-------------------------|--|
| Tipo de conector | |
|-------------------------|--|

| | |
|-------------|---------|
| SFP+ a SFP+ | Exigido |
|-------------|---------|

| | |
|----------------------------------|--|
| Radio mínimo de curvatura | |
|----------------------------------|--|

| | |
|--------------------|---------|
| 7.5mm, Como minimo | Exigido |
|--------------------|---------|

| | | | | |
|---|-------------------|---------------------------|--|---|
| 3 | SUS ACCESORIOS | activo (AOC) 10G SFP + | Chaqueta | 2 |
| | | | OFNP | |
| | | | Directivas | |
| | | | 1x InfiniBand QDR, DDR, SDR, 10G Gigabit Ethernet, Canal de fibra. | |
| | | | Velocidad máxima de datos | |
| | | | 10Gbps | |
| | | | Longitud de cable | |
| | | | 1m (3.28ft) | |
| | | | Rango de Temperatura. | |
| | | | 0 a 70°C | |
| | | | Requerimientos Mínimos | |
| | | | Compatible | |
| | | | Marca y Modelo Switch | |
| | | | Factor de forma | |
| | | | SFP+ | |
| | | | Distancia máxima de cable | |
| | | | Up a 80m, Como mínimo | |
| | | | Conector | |
| | | | RJ-45, Como minimo | |
| | | | Velocidad máxima de datos | |
| | | | 10Gbps | |
| | | | Consumo de energía | |
| | | | 1.8W | |
| | | | Función de DOM | |
| | | | No soportado | |
| | | | Protocolos | |
| | | | De conformidad con SFP+ MSA, CPRI, eCPRI | |
| | | | Rango de Temperatura. | |
| | | | 0 a 70°C, Como minimo | |
| | | | Requerimientos Mínimos | |
| | | | Compatible | |
| | | | Marca y Modelo Switch | |
| | | | Factor de forma | |
| | | | SFP+ | |
| | | | Longitud de onda | |
| | | | | |

| | | | | | |
|---|------------------------------------|--------------------------------------|---|---------|---|
| | | | 850nm, Como mínimo | Exigido | |
| | | | Conector | | |
| | | | LC dúplex | Exigido | |
| 5 | DATA CENTER Y SUS ACCESORIOS | 10GBASE-SR SFP+ 850nm 300m DOM | Velocidad máxima de datos | | 8 |
| | | | 10.3125Gbps, Como minimo | Exigido | |
| | | | Consumo de energía | | |
| | | | ≤0.6W, Como minimo | Exigido | |
| | | | Función de DOM | | |
| | | | Soportado | Exigido | |
| | | | Protocolos | | |
| | | | De conformidad con SFP + MSA, IEEE 802.3ae, SFF-8472, SFF-8431, SFF-8432, CPRI, eCPRI | Exigido | |
| | | | Rango de Temperatura. | | |
| | | | 0 a 70°C, Como minimo | Exigido | |

LOTE 2

Software de Seguridad y Control de Punto Final

500 licencias por un período de 24 meses

Especificaciones técnicas

1. Servidor de Administración y Consola Administrativa

1. Compatibilidad:

- Microsoft Windows 10 20H2 32 bits o 64 bits (versiones 12.2 en adelante).
- Microsoft Windows 10 20H1 32 bits o 64 bits (versiones 12.1 en adelante).
- Microsoft Windows 10 Enterprise 2019 LTSC 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 2016 LTSC 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 2015 LTSC 32 bits / 64 bits.
- Microsoft Windows 10 Pro RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits.
- Microsoft Windows 10 Pro para estaciones de trabajo RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits.
- Microsoft Windows 10 Enterprise RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits.
- Microsoft Windows 10 Education RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits.
- Microsoft Windows 10 Pro 19H1 32 bits / 64 bits.
- Microsoft Windows 10 Pro for Workstations 19H1 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 19H1 32 bits / 64 bits.
- Microsoft Windows 10 Education 19H1 32 bits / 64 bits.
- Microsoft Windows 10 Pro 19H2 32 bits / 64 bits.
- Microsoft Windows 10 Pro for Workstations 19H2 32 bits / 64 bits.
- Microsoft Windows 10 Enterprise 19H2 32 bits / 64 bits.
- Microsoft Windows 10 Education 19H2 32 bits / 64 bits.
- Microsoft Windows 8.1 Pro 32 bits / 64 bits.
- Microsoft Windows 8.1 Enterprise 32 bits / 64 bits.
- Microsoft Windows 8 Pro 32 bits / 64 bits.
- Microsoft Windows 8 Enterprise 32 bits / 64 bits.
- Microsoft Windows 7 Professional con Service Pack 1 y versiones posteriores 32 bits / 64 bits.
- Microsoft Windows 7 Enterprise / Ultimate con Service Pack 1 y versiones posteriores 32 bits / 64 bits.
- Windows Server 2019 Standard 64 bits.
- Windows Server 2019 Core 64 bits.
- Windows Server 2019 Datacenter 64 bits.
- Windows Server 2016 Server Standard RS3 (v1709) (LTSC / CBB) 64 bits.
- Windows Server 2016 Server Datacenter RS3 (v1709) (LTSC / CBB) 64 bits.
- Windows Server 2016 Server Core RS3 (v1709)
- Windows Server 2016 Standard (LTSC) 64 bits.
- Windows Server 2016 Server Core
- Windows Server 2016 Datacenter (LTSC) 64 bits.
- Windows Server 2012 R2 Standard 64 bits.
- Windows Server 2012 R2 Server Core 64 bits.
- Windows Server 2012 R2 Foundation 64 bits.

36. Windows Server 2012 R2 Essentials 64 bits.
37. Windows Server 2012 R2 Datacenter 64 bits.
38. Windows Server 2012 Standard 64 bits.
39. Windows Server 2012 Server Core 64 bits.
40. Windows Server 2012 Foundation 64 bits.
41. Windows Server 2012 Essentials 64 bits.
42. Windows Server 2012 Datacenter 64 bits.
43. Windows Storage Server 2016 64 bits.
44. Windows Storage Server 2012 R2 64 bits.
45. Windows Storage Server 2012 64 bit

2. Características:

1. Se debe acceder a la consola vía WEB (HTTPS) o MMC;
2. Compatibilidad con Windows FailoverClustering u otra solución de alta disponibilidad
3. Capacidad de eliminar remotamente cualquier solución antivirus (propia o de terceros) que esté presente en las estaciones y servidores, sin la necesidad de la contraseña de remoción del actual antivirus;
4. Capacidad de instalar remotamente la solución de antivirus en las estaciones y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory;
5. Capacidad de instalar remotamente la solución de seguridad en smartphones y Android, utilizando estaciones como intermediadoras;
6. Capacidad de instalar remotamente la solución de seguridad en smartphones y tablets de sistema iOS;
7. Capacidad de instalar remotamente cualquier app en smartphones y tablets de sistema iOS;
8. Capacidad de gestionar estaciones de trabajo y servidores de archivos (tanto Windows como Linux y Mac) protegidos por la solución antivirus;
9. Capacidad de gestionar smartphones y tablets (tanto Symbian como Windows Mobile, BlackBerry, Android y iOS) protegidos por la solución antivirus;
10. Capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto;
11. Capacidad de actualizar los paquetes de instalación con las últimas vacunas, para que cuando el paquete sea utilizado en una instalación ya contenga las últimas vacunas lanzadas;
12. Capacidad de hacer distribución remota de cualquier software, o sea, debe ser capaz de remotamente enviar cualquier software por la estructura de gerenciamiento de antivirus para que sea instalado en las máquinas clientes;
13. Capacidad de desinstalar remotamente cualquier software instalado en las máquinas clientes;
14. Capacidad de aplicar actualizaciones de Windows remotamente en las estaciones y servidores;
15. Capacidad de importar la estructura de Active Directory para encontrar máquinas;
16. Capacidad de monitorear diferentes subnets de red con el objetivo de encontrar máquinas nuevas para que sean agregadas a la protección;
17. Capacidad de monitorear grupos de trabajos ya existentes y cualquier grupo de trabajo que sea creado en la red, a fin de encontrar máquinas nuevas para ser agregadas a la protección;
18. Capacidad de, al detectar máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antivirus instalado. En caso de no tenerlo, debe instalar el antivirus automáticamente;
19. Capacidad de agrupamiento de máquinas por características comunes entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antivirus instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 2 días, etc.;
20. Capacidad de definir políticas de configuraciones diferentes por grupos de estaciones, permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos;
21. Debe proporcionar las siguientes informaciones de las computadoras:
 1. Si el antivirus está instalado;
 2. Si el antivirus ha iniciado;
 3. Si el antivirus está actualizado;
 4. Minutos/horas desde la última conexión de la máquina con el servidor administrativo;
 5. Minutos/horas desde la última actualización de vacunas
 6. Fecha y horario de la última verificación ejecutada en la máquina;
 7. Versión del antivirus instalado en la máquina;
 8. Si es necesario reiniciar la computadora para aplicar cambios;
 9. Fecha y horario de cuando la máquina fue encendida;
 10. Cantidad de virus encontrados (contador) en la máquina;
 11. Nombre de la computadora;
 12. Dominio o grupo de trabajo de la computadora;
 13. Fecha y horario de la última actualización de vacunas;
 14. Sistema operativo con Service Pack;
 15. Cantidad de procesadores;
 16. Cantidad de memoria RAM;
 17. Usuario(s) conectados en ese momento, con información de contacto (si están disponibles en el Active Directory)
 18. Dirección IP;
 19. Aplicativos instalados, inclusive aplicativos de terceros, con historial de instalación, conteniendo fecha y hora que el software fue instalado o removido.
 20. Actualizaciones de Windows Updates instaladas
 21. Información completa de hardware conteniendo: procesadores, memoria, adaptadores de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD
 22. Vulnerabilidades de aplicativos instalados en la máquina
22. Debe permitir bloquear las configuraciones del antivirus instalado en las estaciones y servidores de manera que el usuario no consiga modificarlas;
23. Capacidad de reconectar máquinas clientes al servidor administrativo más próximo, basado en reglas de conexión como:
 1. Cambio de gateway;
 2. Cambio de subnet DNS;
 3. Cambio de dominio;
 4. Cambio de servidor DHCP;
 5. Cambio de servidor DNS;

6. Cambio de servidor WINS;
7. Aparición de nueva subnet;
24. Capacidad de configurar políticas móviles para que cuando una computadora cliente esté fuera de la estructura de protección pueda actualizarse vía internet;
25. Capacidad de instalar otros servidores administrativos para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes;
26. Capacidad de interrelacionar servidores en estructura de jerarquía para obtener informes sobre toda la estructura de antivirus;
27. Capacidad de herencia de tareas y políticas en la estructura jerárquica de servidores administrativos;
28. Capacidad de elegir cualquier computadora cliente como repositorio de vacunas y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red;
29. Capacidad de hacer de este repositorio de vacunas un gateway para conexión con el servidor de administración, para que otras máquinas que no logran conectarse directamente al servidor puedan usar este gateway para recibir y enviar informaciones al servidor administrativo.
30. Capacidad de exportar informes para los siguientes tipos de archivos: PDF, HTML y XML.
31. Capacidad de generar traps SNMP para monitoreo de eventos;
32. Capacidad de enviar correos electrónicos para cuentas específicas en caso de algún evento;
33. Debe tener compatibilidad con Microsoft NAP, cuando se instale en Windows 2008 Server;
34. Debe tener compatibilidad con Cisco Network Admission Control (NAC);
35. Debe tener documentación de la estructura del banco de datos para generación de informes a partir de herramientas específicas de consulta (CrystalReports, por ejemplo).
36. Capacidad de conectar máquinas vía Wake on Lan para realización de tareas (barrido, actualización, instalación, etc.), inclusive de máquinas que estén en subnets diferentes del servidor);
37. Capacidad de habilitar automáticamente una política en caso de que ocurra una epidemia en la red (basado en cantidad de virus encontrados en determinado intervalo de tiempo);
38. Capacidad de realizar actualización incremental de vacunas en las computadoras clientes;
39. Capacidad de reportar vulnerabilidades de software presentes en las computadoras.
40. Capacidad de realizar inventario de hardware de todas las máquinas clientes;
41. Capacidad de realizar inventario de aplicativos de todas las máquinas clientes;
42. Capacidad de diferenciar máquinas virtuales de máquinas físicas;

3. Estaciones Windows

1. Compatibilidad:

1. Windows 10
2. Windows 8.1
3. Windows 8
4. Windows 7 todas las versiones, Service Pack 1 o superior

2. Características:

1. Debe proporcionar las siguientes protecciones:
 1. Antivirus de archivos residente (antispysware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
 2. Antivirus de web (módulo para verificación de sitios y downloads contra virus)
 3. Antivirus de correo electrónico (módulo para verificación de correos recibidos y enviados, así como sus adjuntos)
 4. Antivirus de mensajes instantáneos (módulo para verificación de mensajes instantáneos, como ICQ, MSN, IRC, etc.)
 5. Firewall con IDS
 6. Autoprotección (contra ataques a los servicios/procesos del antivirus)
 7. Control de dispositivos externos
 8. Control de acceso a sitios por categoría
 9. Control de ejecución de aplicativos
 10. Control de vulnerabilidades de Windows y de los aplicativos instalados
2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota;
3. Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo).
4. Capacidad de automáticamente deshabilitar el Firewall de Windows (en caso de que exista) durante la instalación, para evitar incompatibilidad con el Firewall de la solución;
5. Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación;
6. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, (ej.: Win32.Trojan.banker) para que cualquier objeto detectado con el resultado elegido sea ignorado;
7. Capacidad de agregar aplicativos a una lista de aplicativos confiables, donde las actividades de red, actividades de disco y acceso al registro de Windows no serán monitoreadas;
8. Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks);
9. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;
10. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;
11. Capacidad de verificar solamente archivos nuevos y modificados;
12. Capacidad de verificar objetos usando heurística;
13. Capacidad de agendar una pausa en la verificación;
14. Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo;
15. El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe:
 1. Preguntar qué hacer, o;
 2. Bloquear el acceso al objeto;
 1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador);

2. Caso positivo de desinfección:
 1. Recuperar el objeto para uso;
3. Caso negativo de desinfección:
 1. Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador);
16. Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto.
17. Capacidad de verificar correos electrónicos recibidos y enviados en los protocolos POP3, IMAP, NNTP, SMTP y MAPI, así como conexiones cifradas (SSL) para POP3 y IMAP (SSL);
18. Capacidad de verificar tráfico de ICQ, MSN, AIM y IRC contra virus y enlaces phishings;
19. Capacidad de verificar enlaces introducidos en correos electrónicos contra pishings;
20. Capacidad de verificar tráfico SSL en los browsers: Internet Explorer, Firefox y Opera;
21. Capacidad de verificación del cuerpo del correo electrónico y adjuntos usando heurística;
22. El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe:
 1. Preguntar qué hacer, o;
 2. Bloquear el correo electrónico;
 1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador);
 2. Caso positivo de desinfección:
 1. Recuperar el correo electrónico al usuario;
 3. Caso negativo de desinfección:
 1. Mover a cuarentena o borrar el objeto (de acuerdo con la configuración preestablecida por el administrador);
23. En caso de que el correo electrónico contenga código que parece ser, pero no es definitivamente malicioso, este debe mantenerse en cuarentena.
24. Posibilidad de verificar solamente correos electrónicos recibidos, o recibidos y enviados.
25. Capacidad de filtrar adjuntos de correos electrónicos, borrándolos o renombrándolos de acuerdo con la configuración hecha por el administrador.
26. Capacidad de verificación de tráfico HTTP y cualquier script de Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;
27. Debe tener soporte total al protocolo IPv6;
28. Capacidad de modificar las puertas monitoreadas por los módulos de web y correo electrónico;
29. En la verificación de tráfico web, en caso de que se encuentre código malicioso el programa debe:
 1. Preguntar qué hacer, o;
 2. Bloquear el acceso al objeto y mostrar un mensaje sobre el bloqueo, o;
 3. Permitir acceso al objeto;
30. El antivirus de web debe realizar la verificación de, como mínimo, dos maneras diferentes, a elección del administrador:
 1. Verificación *on-the-fly*, donde los datos se verifican mientras son recibidos en tiempo real, o;
 2. Verificación de *buffer*, donde los datos se reciben y son almacenados para posterior verificación.
31. Posibilidad de agregar sitios de la web en una lista de exclusión, donde no serán verificados por el antivirus de web.
32. Debe contar con módulo que analice las acciones de cada aplicación en ejecución en la computadora, grabando las acciones ejecutadas y comparándolas con secuencias características de actividades peligrosas. Tales registros de secuencias deben ser actualizados conjuntamente con las vacunas.
33. Debe contar con módulo que analice cada macro de VBA ejecutado, buscando señales de actividad maliciosa.
34. Debe contar con módulo que analice cualquier intento de edición, exclusión o grabación del registro, de forma que sea posible elegir claves específicas para ser monitoreadas y/o bloqueadas.
35. Debe tener módulo de bloqueo de *Phishing*, con actualizaciones incluidas en las vacunas, obtenidas por *Anti-PhishingWorkingGroup* (<http://www.antiphishing.org/>).
36. Capacidad de distinguir diferentes subnets y brindar opción de activar o no el firewall para una subnet específica;
37. Debe tener módulo IDS (*IntrusionDetectionSystem*) para protección contra *portscans* y exploración de vulnerabilidades de software. La base de datos de análisis debe actualizarse conjuntamente con las vacunas.
38. El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:
 1. Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas;
 2. Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados.
39. Debe tener módulo que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínimo:
 1. Discos de almacenamiento locales
 2. Almacenamiento extraíble
 3. Impresoras
 4. CD/DVD
 5. Drives de disquete
 6. Modems
 7. Dispositivos de cinta
 8. Dispositivos multifuncionales
 9. Lectores de smart card
 10. Dispositivos de sincronización vía ActiveSync (Windows CE, Windows Mobile, etc.)
 11. Wi-Fi
 12. Adaptadores de red externos
 13. Dispositivos MP3 o smartphones
 14. Dispositivos Bluetooth
40. Capacidad de liberar acceso a un dispositivo específico y usuarios específicos por un período de tiempo específico, sin la necesidad de deshabilitar la protección, sin deshabilitar el gerenciamento central o de intervención local del administrador en la máquina del usuario.
41. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por usuario.
42. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por agendamiento.
43. Capacidad de configurar nuevos dispositivos por Class ID/Hardware ID
44. Capacidad de limitar el acceso a sitios de internet por categoría, por contenido (video, audio, etc.), con posibilidad de configuración por usuario o grupos de usuarios y agendamiento.
45. Capacidad de limitar la ejecución de aplicativos por hash MD5, nombre del archivo, versión del archivo, nombre del aplicativo, versión del aplicativo, fabricante/desarrollador, categoría (ej.: navegadores, gerenciador de download, juegos, aplicación de acceso remoto,

- etc.).
 - 46. Capacidad de bloquear la ejecución de un aplicativo que esté en almacenamiento externo.
 - 47. Capacidad de limitar el acceso de los aplicativos a recursos del sistema, como claves de registro y carpetas/archivos del sistema, por categoría, fabricante o nivel de confianza del aplicativo.
 - 48. Capacidad de, en caso de epidemia, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.
 - 49. Capacidad de, en caso de que la computadora cliente salga de la red corporativa, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.
4. Estaciones y Servidores Mac OS X
- 1. Compatibilidad:
 - 1. Mac OS X 10.12 o superior
 - 2. Mac OS X Server 10.9 o superior
 - 2. Características:
 - 1. Debe proporcionar protección residente para archivos (antispysware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
 - 2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota;
 - 3. La instalación y primera ejecución del producto debe ser realizada sin necesidad de reiniciar la computadora, de modo que el producto funcione en toda su capacidad;
 - 4. Debe contar con soportes a notificaciones utilizando Growl;
 - 5. Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo).
 - 6. Capacidad de volver a la base de datos de la vacuna anterior;
 - 7. Capacidad de barrer la cuarentena automáticamente después de cada actualización de vacunas;
 - 8. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, (ej.: Win32.Trojan.banker) para que cualquier objeto detectado con el resultado elegido sea ignorado;
 - 9. Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks);
 - 10. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;
 - 11. Capacidad de verificar solamente archivos nuevos y modificados;
 - 12. Capacidad de verificar objetos usando heurística;
 - 13. Capacidad de agendar una pausa en la verificación;
 - 14. El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe:
 - 1. Preguntar qué hacer, o;
 - 2. Bloquear el acceso al objeto;
 - 1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador);
 - 2. Caso positivo de desinfección:
 - 1. Recuperar el objeto para uso;
 - 3. Caso negativo de desinfección:
 - 1. Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador);
 - 15. Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto;
 - 16. Capacidad de verificar archivos de formato de correo electrónico;
 - 17. Posibilidad de trabajar con el producto por la línea de comando, con como mínimo opciones para actualizar las vacunas, iniciar un barrido, para el antivirus e iniciar el antivirus por la línea de comando;
 - 18. Capacidad de ser instalado, removido y administrado por la misma consola central de gestión;
5. Estaciones de trabajo Linux
- 1. Compatibilidad:
 - 1. Debian GNU / Linux 8.9 o superior, x86 / x64
 - 2. Ubuntu 16.04 LTS o superior, x86 / x64
 - 3. Linux Mint 18.2 o superior, x86 / x64
 - 4. ALT, x86 / x64
 - 5. GosLinux 6.6 o superior, x86 / x64
 - 6. Mageia 4, x86
 - 7. Amazon Linux AMI, x64
 - 8. Astra Linux, x64
 - 9. OS ROSA Cobalt, x64
 - 10. AlterOS 7.5 o superior, x64
 - 11. Pardus OS 19.1 o superior, x64
 - 2. Características:
 - 1. Debe proporcionar las siguientes protecciones:
 - 1. Antivirus de archivos residente (antispysware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
 - 2. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.
 - 2. Capacidad de configurar el permiso de acceso a las funciones del antivirus con, como mínimo, opciones para las siguientes funciones:

1. Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);
2. Gerenciamiento de respaldo: Creación de copias de los objetos infectados en un reservorio de respaldo antes del intento de desinfectar o eliminar tal objeto, siendo de esta manera posible la recuperación de objetos que contengan informaciones importantes;
3. Gerenciamiento de cuarentena: Cuarentena de objetos sospechosos y corrompidos, guardando tales archivos en una carpeta de cuarentena;
4. Verificación por agendamiento: búsqueda de archivos infectados y sospechosos (incluyendo archivos dentro de un rango especificado); análisis de archivos; desinfección o eliminación de objetos infectados.
3. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otros software;
4. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;
5. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;
6. Capacidad de verificar objetos usando heurística;
7. Posibilidad de elegir la carpeta donde los archivos recuperados de respaldo y los archivos se grabarán
8. Posibilidad de elegir la carpeta donde se guardarán los respaldos y archivos en cuarentena
9. Debe contar con módulo de administración remoto a través de herramienta nativa o Webmin (herramienta nativa GNU-Linux)

6. Servidores Windows

1. Compatibilidad:

1. Windows Server 2019 todas las versiones
2. Windows Server 2016 todas las versiones
3. Windows Server 2012 todas las versiones
4. Windows Server 2008 todas las versiones, Service Pack 1 o superior
5. Windows Server 2003 todas las versiones, Service Pack 2 o superior
6. Windows Storage Server 2012 o superior
7. Hyper-V Server 2012 o superior
8. Windows MultiPoint Server 2011 o superior
9. Small Business Server 2008 o superior

2. Características:

1. Debe proporcionar las siguientes protecciones:
 1. Antivirus de archivos residente (antispysware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
 2. Autoprotección contra ataques a los servicios/procesos del antivirus
 3. Firewall con IDS
 4. Control de vulnerabilidades de Windows y de los aplicativos instalados
2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota;
3. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.
4. Capacidad de configurar el permiso de acceso a las funciones del antivirus con, como mínimo, opciones para las siguientes funciones:
 1. Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);
 2. Gerenciamiento de tarea (crear o excluir tareas de verificación)
 3. Lectura de configuraciones
 4. Modificación de configuraciones
 5. Gerenciamiento de respaldo y cuarentena
 6. Visualización de informes
 7. Gerenciamiento de informes
 8. Gerenciamiento de claves de licencia
 9. Gerenciamiento de permisos (agregar/excluir permisos superiores)
5. El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:
 1. Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas;
 2. Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados.
6. Capacidad de seleccionar por separado el número de procesos que ejecutarán funciones de barrido en tiempo real, el número de procesos que ejecutarán el barrido a demanda y el número máximo de procesos que pueden ser ejecutados en total.
7. Capacidad de reanudar automáticamente tareas de verificación que hayan sido interrumpidas por anomalías (corte de energía, errores, etc.)
8. Capacidad de automáticamente pausar y no iniciar tareas agendadas en caso de que el servidor esté funcionando con fuente ininterrumpida de energía (*uninterruptible Powersupply UPS*)
9. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otros software;
10. Capacidad de configurar niveles de verificación diferentes para cada carpeta, grupo de carpetas o archivos del servidor.
11. Capacidad de bloquear acceso al servidor de máquinas infectadas y cuando una máquina intenta grabar un archivo infectado en el servidor.
12. Capacidad de crear una lista de máquinas que nunca serán bloqueadas aunque sean infectadas.
13. Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación;
14. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, (ej.: Win32.Trojan.banker) para que cualquier objeto detectado con el resultado elegido sea ignorado;
15. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;
16. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;
17. Capacidad de verificar solamente archivos nuevos y modificados;

18. Capacidad de elegir qué tipo de objeto compuesto será verificado (ej.: archivos comprimidos, archivos autodescompresores, .PST, archivos compactados por compactadores binarios, etc.)
19. Capacidad de verificar objetos usando heurística;
20. Capacidad de configurar diferentes acciones para diferentes tipos de amenazas;
21. Capacidad de agendar una pausa en la verificación;
22. Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo;
23. El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe:
 1. Preguntar qué hacer, o;
 2. Bloquear el acceso al objeto;
 1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador);
 2. Caso positivo de desinfección:
 1. Recuperar el objeto para uso;
 3. Caso negativo de desinfección:
 1. Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador);
24. Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto.
25. Posibilidad de elegir la carpeta donde los archivos recuperados de respaldo y los archivos se grabarán
26. Posibilidad de elegir la carpeta donde se guardarán los respaldos y archivos en cuarentena
27. Debe contar con módulo que analice cada script ejecutado, buscando señales de actividad maliciosa.

7. Servidores Linux

1. Compatibilidad:

1. CentOS 6.7 o superior, x86 / x64
2. Red Hat® Enterprise Linux® 6.7 o superior, x64
3. Oracle Linux 7.3 o superior, x64

2. Características:

1. Debe proporcionar las siguientes protecciones:
 1. Antivirus de archivos residente (antispymware, antitroyano, antimallware, etc.) que verifique cualquier archivo creado, accedido o modificado;
 2. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.
2. Capacidad de configurar el permiso de acceso a las funciones del antivirus con, como mínimo, opciones para las siguientes funciones:
 1. Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);
 2. Gerenciamiento de respaldo: Creación de copias de los objetos infectados en un reservorio de respaldo antes del intento de desinfectar o eliminar tal objeto, siendo de esta manera posible la recuperación de objetos que contengan informaciones importantes;
 3. Gerenciamiento de cuarentena: Cuarentena de objetos sospechosos y corrompidos, guardando tales archivos en una carpeta de cuarentena;
 4. Verificación por agendamiento: búsqueda de archivos infectados y sospechosos (incluyendo archivos dentro de un rango especificado); análisis de archivos; desinfección o eliminación de objetos infectados.
3. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otro software;
4. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;
5. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;
6. Capacidad de verificar objetos usando heurística;
7. Posibilidad de elegir la carpeta donde los archivos recuperados de respaldo y los archivos se grabarán
8. Posibilidad de elegir la carpeta donde se guardarán los respaldos y archivos en cuarentena
9. Debe contar con módulo de administración remoto a través de herramienta nativa o Webmin (herramienta nativa GNU-Linux)

7. Smartphones y tablets-

1. Compatibilidad:

1. Apple iOS 10.0 o superior
2. Android OS 4.2 o superior

2. Características:

1. Debe proporcionar las siguientes protecciones:
 1. Protección en tiempo real del sistema de archivos del dispositivo — interceptación y verificación de:
 1. Todos los objetos transmitidos usando conexiones wireless (puerta de infrarrojo, Bluetooth) y mensajes EMS, durante sincronismo con PC y al realizar descargas usando el browser.
 2. Archivos abiertos en el smartphone
 3. Programas instalados usando la interface del smartphone
 2. Verificación de los objetos en la memoria interna del smartphone y en las tarjetas de expansión a pedido del usuario y de acuerdo con un agendamiento;
2. Deberá aislar en área de cuarentena los archivos infectados;
3. Deberá actualizar las bases de vacunas de modo agendado;
4. Deberá bloquear spam de SMS a través de Black lists (listas negras);
5. Deberá tener función de bloqueo del aparato en caso de que la SIM CARD sea cambiada por otra no autorizada;
6. Deberá tener función de limpieza de datos personales a distancia, en caso de robo, por ejemplo.
7. Deberá tener firewall personal;
8. Posibilidad de instalación remota utilizando Microsoft System Center Mobile Device Manager 2008 SP1
9. Posibilidad de instalación remota utilizando SybaseAfaría 6.5

10. Capacidad de detectar Jailbreak en dispositivos iOS
11. Capacidad de bloquear el acceso a sitios por categoría en dispositivos
12. Capacidad de bloquear el acceso a sitios phishing o maliciosos
13. Capacidad de crear contenedores de aplicativos, separando datos corporativos de datos personales
14. Capacidad de configurar white y blacklist (listas blancas y listas negras) de aplicativos

8. Manejo de dispositivos móviles (MDM):

1. Compatibilidad:
 1. Dispositivos conectados a través de Microsoft Exchange ActiveSync
 1. Apple iOS
 2. Android
 2. Dispositivos con soporte a Apple Push Notification (APNs) service
 1. Apple iOS 11.0 o superior
2. Características:
 1. Capacidad de aplicar políticas de ActiveSync a través del servidor Microsoft Exchange
 2. Capacidad de ajustar las configuraciones de:
 1. Sincronización de correo electrónico
 2. Uso de aplicativos
 3. Contraseña del usuario
 4. Cifrado de datos
 5. Conexión de medios extraíbles
 3. Capacidad de instalar certificados digitales en dispositivos móviles
 4. Capacidad de, en forma remota, resetear la contraseña de dispositivos iOS
 5. Capacidad de, en forma remota, borrar todos los datos de dispositivos iOS
 6. Capacidad de, en forma remota, bloquear un dispositivo iOS

9. Cifrado:

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

10. Gerenciamiento de Sistemas:

1. Capacidad de crear imágenes de sistema operativo remotamente y distribuir esas imágenes para computadoras gestionadas por la solución y para computadoras *bare-metal*.
2. Capacidad de detectar software de terceros vulnerables, creando así un informe de software vulnerables.
3. Capacidad de corregir las vulnerabilidades de software, haciendo el download centralizado de la corrección o actualización y aplicando esa corrección o actualización en las máquinas gestionadas de manera transparente para los usuarios.
4. Contar con tecnología de Control de Admisión de Red (NAC), con la posibilidad de crear reglas de qué tipos de dispositivos pueden tener accesos a recursos de la red.
5. Capacidad de gestionar licencias de software de terceros.
6. Capacidad de registrar cambios de hardware en las máquinas gestionadas.
7. Capacidad de gestionar un inventario de hardware, con la posibilidad de registro de dispositivos (ej.: router, switch, proyector, accesorio, etc.), informando fecha de compra, lugar donde se encuentra, servicetag, número de identificación y otros.

11. Servidores de correo electrónico Windows

1. Características:
 1. Debe utilizar las tecnologías VSAPI 2.0, 2.5 y 2.6;
 2. Capacidad de iniciar varias copias del proceso de antivirus;
 3. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.
 4. Capacidad de verificar carpetas públicas, correos electrónicos enviados, recibidos y almacenados contra virus, spywares, adwares, gusanos, troyanos y riskwares;
 5. Capacidad de verificar carpetas públicas y correos electrónicos almacenados de forma agendada, utilizando las últimas vacunas y heurística;

6. El antivirus, al encontrar un objeto infectado, debe:
 1. Desinfectar el objeto, notificando el remitente, destinatario y administradores, o
 2. Excluir el objeto, sustituyéndolo por una notificación;
 3. Bloquear el acceso al objeto;
 1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador);
 2. Caso positivo de desinfección:
 1. Recuperar el objeto para uso;
 3. Caso negativo de desinfección:
 1. Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador);
7. Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto.
8. Capacidad de enviar notificaciones sobre virus detectados para el administrador, para el destinatario y remitente del mensaje infectado.
9. Capacidad de grabar logs de actividad de virus en los eventos del sistema y en los logs internos de la aplicación;
10. Capacidad de detectar diseminación en masa de correos infectados, informando al administrador y registrando tales eventos en los logs del sistema y de la aplicación.

12. Servidores de correo electrónico Lotus Notes/Domino

1. Características:
 1. Capacidad de barrido de banco de datos internos del sistema Lotus Notes/Domino;
 2. Capacidad de barrido en las réplicas de otros servidores Domino que no tengan el antivirus instalado;
 3. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.
 4. Capacidad de barrido de virus en todos los correos electrónicos que pasan por el sistema Lotus Notes/Domino;
 5. El barrido debe involucrar el texto del mensaje y los archivos adjuntos;
 6. Capacidad de cura de mensajes infectados;
 7. Capacidad de filtrado de archivos por tipo;
 8. Capacidad de creación de cuarentena para objetos sospechosos, evitando pérdida de datos;
 9. Capacidad de notificación del destinatario, remitente y administrador sobre objetos que contengan archivos maliciosos;
 10. Capacidad de detección de epidemias y notificaciones de estos eventos al administrador;
 11. Capacidad de actualización vía HTTP, FTP o carpeta en red local;
 12. Capacidad de configurar el tamaño máximo de un archivo que será verificado;

13. Servidores de correo electrónico Linux:

1. Características:
 1. Capacidad de verificar el tráfico SMTP del servidor contra malware en todos los elementos del correo electrónico: encabezado, cuerpo y adjunto;
 2. Capacidad de notificar al administrador, al remitente y al destinatario en caso de que un archivo malicioso sea encontrado en el correo electrónico;
 3. Capacidad de poner en cuarentena objetos maliciosos;
 4. Capacidad de guardar respaldo de los objetos antes del intento de desinfección;
 5. Capacidad de hacer barrido en el sistema de archivos del servidor;
 6. Capacidad de filtrar adjuntos por nombre o tipo de archivo;
 7. Capacidad de crear grupos de usuarios para aplicar reglas de verificación de correos electrónicos;
 8. Debe permitir gestión vía consola WEB;
 9. Debe ser actualizado de manera automática vía internet o por servidores locales, con frecuencia horaria.

14. Servidores de gateway

Características:

1. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.
2. Capacidad de verificar tráfico HTTP 1.0 y 1.1 (RFC 2616), FTP (RFC 959, 2389, Extensiones para FTP) y FTP sobre HTTP;
3. Capacidad de definir listas de tipos de objetos que no serán verificados;
4. Capacidad de definir listas de servidores a los cuales no se les verificará el tráfico;
5. Capacidad de crear grupos de usuarios y aplicar reglas de verificación por grupos;
6. Capacidad de iniciar varias copias del proceso de antivirus;
7. Capacidad de elegir el tamaño reservado en la memoria para almacenamiento de los archivos que serán verificados;
8. Capacidad de elegir el tamaño del buffer del archivo que será verificado;
9. Capacidad de elegir el número máximo de objetos en la fila de verificación;
10. Capacidad de definir el tiempo máximo de verificación de un objeto;

Términos a tener en cuenta:

1. Contar como mínimo con 3 ingenieros certificados con las certificaciones avanzadas del producto
2. contar como mínimo con 2 técnicos con certificaciones de cifrado
3. Contar con por lo menos 2 técnicos con certificaciones en protección de servidores de correo antispam
4. Contar con por lo menos 2 técnicos con certificaciones en Detecciones y Respuesta de Endpoints.
5. Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar certificados de inscripción en IPS
6. contar como mínimo con 3 ingenieros con certificaciones ITIL para garantizar la buena asistencia en soporte técnico.
7. contar con al menos 10 contratos o facturas de la provisión del Software ofertado entre los años 2018, 2019 y 2020.
8. implementación de todos los módulos de la herramienta en todo el parque de equipos.
9. capacitación de la herramienta a todas las personas involucradas en el departamento de tecnología.
10. soporte técnico incluido durante todo el periodo de licenciamiento.
11. cantidad de tickets de soporte ilimitados.
12. El proveedor deberá ser Canal Platinum de la Marca ofertada, para garantizar el buen servicio y respaldo del soporte local, para ello deberá

presentar el certificado que lo avale.

13. El proveedor deberá tener la Certificación ISO 9001 Sistema de Gestión de Calidad y la Certificación ISO 27001 Sistema de Gestión de Seguridad de la Información para garantizar el buen servicio y respaldo del soporte local.
14. El proveedor deberá presentar con su oferta una Carta de autorización del fabricante expresamente dirigido a la convocante refiriendo el nro. de ID del llamado
15. El proveedor deberá contar con una plataforma y/o sistema de ticket para atención de casos de soporte técnico, a fin de garantizar la respuesta de manera profesional y organizada.
16. El proveedor local deberá contar con una plataforma de autoservicio de preguntas frecuentes, con por lo menos 50 plantillas de respuesta para esos casos, dicha plataforma deberá estar integrada con el sistema del ticket del proveedor

la convocante podrá solicitar si cree necesario a los oferentes una demostración del manejo y despliegue de la herramienta.

Identificación de la unidad solicitante y justificaciones

Nombre, cargo y la dependencia de la Institución de quien solicita el llamado: ANGEL AMARILLA, JEFE, DPTO DE REDES Y SERVIDORES DE LA D.T.I.C.

Necesidad que se pretende satisfacer mediante la contratación a ser realizada: LA DE PROVEER A TODOS NUESTROS EQUIPOS INFORMATICOS LOS SOFTWARES DE SEGURIDAD ANTIVIRUS Y ADQUISICIÓN DE HARDWARE DE RED PARA OPTIMIZAR EL RENDIMIENTO DE NUESTROS EQUIPOS Y EN CONSECUENCIA, LA EFECTIVIDAD EN LA ATENCIÓN A NUESTROS CLIENTES EXTERNOS.

Planificación: SE TRATA DE UN LLAMADO PERIODICO.

Justificar las especificaciones técnicas establecidas: LAS ESPECIFICACIONES TECNICAS RESPONDEN A LA NECESIDAD PARTICULAR DE LA INSTITUCIÓN, DETERMINADAS POR LA D.T.I.C., A FIN DE OPTIMIZAR EL RENDIMIENTO DE LOS EQUIPOS, Y AGILIZAR CON ELLO LAS RESPUESTAS A LA CIUDADANIA.

Plan de entrega de los bienes

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

La firma adjudicada deberá proveer los bienes ante cada pedido realizado al respecto por el Ministerio de Desarrollo Social, mediante las Órdenes de Compra/Servicio emitidas por la Dirección de Tecnología de la Información y Comunicación (DTIC) al el Proveedor.

Una vez recepcionadas las Órdenes de Compra emitidas por la DTIC del MDS, el proveedor contará con 10 (diez) días hábiles para hacer entrega de los bienes solicitados. Los mismos deben ser entregados en la Sede del Ministerio de Desarrollo Social, situado en la Avda. Mariscal López casi Coronel Pampliega, Ciudad de Fernando de la Mora.

Plan de entrega de los servicios

| Ítem | Descripción del servicio | Cantidad | Unidad de medida de los servicios | Lugar donde los servicios serán prestados | Fecha(s) final(es) de ejecución de los servicios |
|-----------------|---|---|--|---|--|
| (Indicar el N°) | (Indicar la descripción de los servicios) | (Insertar la cantidad de rubros de servicios a proveer) | (Indicar la unidad de medida de los rubros de servicios) | (Indicar el nombre del lugar) | (Indicar la(s) fecha(s) de entrega requerida(s)) |
| | | | | | |

CONFORME A LO ESTABLECIDO EN EL APARTADO ANTERIOR.

Planos y diseños

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

No Aplica

Embalajes y documentos

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

No Aplica

Inspecciones y pruebas

Las inspecciones y pruebas serán como se indica a continuación:

No Aplica

Indicadores de Cumplimiento

El documento requerido para acreditar el cumplimiento contractual, será:

Planificación de indicadores de cumplimiento:

| INDICADOR | TIPO | FECHA DE PRESENTACIÓN PREVISTA (se indica la fecha que debe presentar según el PBC) |
|---------------------------------------|---------------------------------------|---|
| Ordenes de Compra / Acta de recepción | Ordenes de Compra / Acta de recepción | Diez días hábiles a partir de la recepción de la Orden de Compra correspondiente. |

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

Criterios de Adjudicación

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

1. La adjudicación en los procesos de contratación en los cuales se aplique la modalidad de contrato abierto, se efectuará por las cantidades o montos máximos solicitados en el llamado, sin que ello implique obligación de la convocante de requerir la provisión de esa cantidad o monto durante 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 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 llamados en los cuales se aplique la modalidad de contrato abierto, cuando la Convocante deba disminuir cantidades o montos a ser adjudicados, no podrá modificar el monto o las cantidades mínimas establecidas en las bases de la contratación.

Notificaciones

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

1. Dentro de los cinco (5) días corridos de haberse resuelto la adjudicación, la convocante comunicará a través del Sistema de Información de Contrataciones Públicas, copia del informe de evaluación y del acto administrativo de adjudicación, los cuales serán puestos a disposición pública en el referido sistema. Adicionalmente el sistema generará una notificación a los oferentes por los medios remotos de comunicación electrónica pertinentes, la cual será reglamentada por la DNCP.
2. En sustitución de la notificación a través del Sistema de Información de Contrataciones Públicas, las convocantes podrán dar a conocer la adjudicación por cédula de notificación a cada uno de los oferentes, acompañados de la copia íntegra del acto administrativo y del informe de evaluación. La no entrega del informe en ocasión de la notificación, suspende el plazo para formular protestas hasta tanto la convocante haga entrega de dicha copia al oferente solicitante.
3. En caso de la convocante opte por la notificación física a los oferentes participantes, deberá realizarse únicamente con el acuse de recibo y en el mismo con expresa mención de haber recibido el informe de evaluación y la resolución de adjudicación.
4. Las cancelaciones o declaraciones desiertas deberán ser notificadas a todos los oferentes, según el procedimiento indicado precedentemente.
5. Las notificaciones realizadas en virtud al contrato, deberán ser por escrito y dirigirse a la dirección indicada en el contrato.

Audiencia Informativa

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

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

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

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

Documentación requerida para la firma del contrato

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

1. Personas Físicas / Jurídicas

- 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.

2. Documentos. Consorcios

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

CONDICIONES CONTRACTUALES

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

Interpretación

Interpretación

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

2. Condiciones prohibidas, inválidas o inejecutables

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

3. Limitación de Dispensas:

a) Toda dispensa a los derechos o facultades de una de las partes en virtud del contrato, deberá ser documentada por escrito, indicar la fecha, estar firmada por un representante autorizado de la parte que otorga dicha dispensa y deberá especificar la obligación que está dispensando y el alcance de la dispensa.

b) Sujeto a lo indicado en el inciso precedente, ningún retraso, prórroga, demora o aprobación por cualquiera de las partes al hacer cumplir algún término y condición del contrato o el otorgar prórrogas por una de las partes a la otra, perjudicará, afectará o limitará los derechos de esa parte en virtud del contrato. Asimismo, ninguna prórroga concedida por cualquiera de las partes por un incumplimiento del contrato, servirá de dispensa para incumplimientos posteriores o continuos del contrato.

Subcontratación

El porcentaje permitido para la subcontratación será de:

No Aplica

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

Derechos Intelectuales

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

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

a) La instalación de los bienes por el proveedor o el uso de los bienes en la República del Paraguay; y

b) La venta de los productos producidos por los bienes en cualquier país.

Dicha indemnización no procederá si los bienes o una parte de ellos fuesen utilizados para fines no previstos en el Contrato o para fines que no pudieran inferirse razonablemente del Contrato. La indemnización tampoco cubrirá cualquier transgresión que resultara del uso de los bienes o parte de ellos, o de cualquier producto producido como resultado de asociación o combinación con otro equipo, planta o materiales no suministrados por el proveedor en virtud del Contrato.

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

4. Si el proveedor no notifica a la contratante dentro de treinta (30) días a partir del recibo de dicha comunicación de su intención de proceder con tales procesos o reclamos, la contratante tendrá derecho a emprender dichas acciones en su propio nombre.
5. La contratante se compromete, a solicitud del proveedor, a prestarle toda la asistencia posible para que el proveedor pueda contestar las citadas acciones legales o reclamaciones. La Contratante será reembolsada por el proveedor por todos los gastos razonables en que hubiera incurrido.
6. La contratante deberá indemnizar y eximir de culpa al proveedor y a sus empleados, funcionarios y subcontratistas, por cualquier litigio, acción legal o procedimiento administrativo, reclamo, demanda, pérdida, daño, costo y gasto, de cualquier naturaleza, incluyendo honorarios y gastos de abogado, que pudieran afectar al proveedor como resultado de cualquier transgresión o supuesta transgresión de patentes, modelos de aparatos, diseños registrados, marcas registradas, derechos de autor, o cualquier otro derecho de propiedad intelectual registrado o ya existente a la fecha del contrato, que pudieran suscitarse con motivo de cualquier diseño, datos, planos, especificaciones, u otros documentos o materiales que hubieran sido suministrados o diseñados por la contratante o a nombre suyo.

Transporte

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

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

No Aplica

Confidencialidad de la información

1. No deberá darse a conocer información alguna acerca del análisis, aclaración y evaluación de las ofertas ni sobre las recomendaciones relativas a la adjudicación, después de la apertura en público de las ofertas, a los oferentes ni a personas no involucradas en el proceso de evaluación, hasta que haya sido dictada la Resolución de Adjudicación 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.
2. La contratante y el proveedor deberán mantener confidencialidad y en ningún momento divulgarán a terceros, sin el consentimiento de la otra parte, documentos, datos u otra información que hubiera sido directa o indirectamente proporcionada por la otra parte en conexión con el Contrato, antes, durante o después de la ejecución del mismo. No obstante, el proveedor podrá proporcionar a sus subcontratistas los documentos, datos e información recibidos de la contratante para que puedan cumplir con su trabajo en virtud del contrato. En tal caso, el proveedor obtendrá de dichos subcontratistas un compromiso de confidencialidad similar al requerido al proveedor en la presente cláusula.

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

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

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

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

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

Obligatoriedad de declarar información del personal del contratista en el SICP

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

2. Cuando ocurra algún cambio en la nómina del personal o de los subcontratistas propuestos, el proveedor o contratista está obligado a actualizar el FIP.
3. Como requerimiento para efectuar los pagos a los proveedores o contratistas, la contratante, a través del procedimiento establecido para el efecto por la entidad previsional, verificará que el proveedor o contratista se encuentre al día en el cumplimiento con sus obligaciones para con el Instituto de Previsión Social (IPS).
4. La Contratante podrá realizar las diligencias que considere necesarias para verificar que la totalidad de las personas que prestan servicios personales en relación de dependencia para la contratista y eventuales subcontratistas se encuentren debidamente individualizados en los listados recibidos.
5. El proveedor o contratista deberá permitir y facilitar los controles de cumplimiento de sus obligaciones de aporte obrero patronal, tanto los que fueran realizados por la contratante como los realizados por el IPS y por funcionarios de la DNCP. La negativa expresa o tácita se considerará incumplimiento del contrato por causa imputable al proveedor o contratista.
6. En caso de detectarse que el proveedor o contratista o alguno de los subcontratistas, no se encontraran al día con el cumplimiento de sus obligaciones para con el IPS, deberán ser emplazados por la contratante para que en diez (10) días hábiles cumplan con sus obligaciones pendientes con la previsional. En el caso de que no lo hiciera, se considerará incumplimiento del contrato por causa imputable al proveedor o contratista.

Formas y condiciones de pago

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

1. Documentos Genéricos:

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

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

Lugar de Presentación de las facturas, será en la Dirección de Tecnología de la Información y Comunicación (DTIC) del MDS, sito en Avda. Mariscal López casi Coronel Pampliega, Ciudad de Fernando de la Mora, de lunes a viernes de 8:00 a 15:00 horas.

La Dirección Administrativa, ante recepción de documentación de pago por parte de la Dirección de Tecnología de la Información y Comunicación (DTIC), cerciorándose de que se han cumplido con todas las exigencias establecidas en el Contrato y las Especificaciones Técnicas establecidas; respecto al plazo expresado en el párrafo anterior, se expedirá sobre las facturas en un plazo no mayor de quince (15) días calendarios de la recepción. Si existiese una diferencia sobre el monto facturado o cualquier inconveniente con los bienes/servicios requeridos, deberá devolver la misma bajo constancia escrita o solicitar una nota de crédito o una factura complementaria.

Así mismo, si los documentos presentados son insuficientes serán devueltos al proveedor bajo constancia escrita para la rectificación correspondiente. En este caso, el plazo para el pago queda interrumpido sin responsabilidad alguna para la Contratante hasta la fecha de presentación de los documentos que cumplan con lo requerido.

Se retendrá en concepto de contribuciones, el equivalente a cero punto cuatro por ciento (0,4 %) sobre el importe de cada factura, deducido los impuestos correspondientes, conforme a lo establecido en el Art. 1° de la Ley 3430/07 que modifica el Artículo 41° de la Ley N° 2051/03.

2. La Contratante efectuará los pagos, dentro del plazo establecido en este apartado, sin exceder sesenta (60) días después de la presentación de una factura por el proveedor, y después de que la contratante la haya aceptado. Dicha aceptación o rechazo, deberá darse a más tardar en quince (15) días posteriores a su presentación.
3. De conformidad a las disposiciones del Decreto N° 7781/2006, del 30 de Junio de 2006 y modificatoria, en las contrataciones con Organismos de la Administración Central, el proveedor deberá habilitar su respectiva cuenta corriente o caja de ahorro en un Banco de plaza y comunicar a la Contratante para que ésta gestione ante la Dirección General del Tesoro Público, la habilitación en el Sistema de Tesorería (SITE).

Solicitud de suspensión de la ejecución del contrato

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

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

Solicitud de Pago de Anticipo

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

No Aplica

Reajuste

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

El ajuste de precios será cuando exista una variación igual o mayor a 15% referente a la fecha de apertura de ofertas y esta se vea reflejada en el Índice de Precios del Consumo (IPC) publicado por el Banco Central del Paraguay.

Formula: $Pr = (Px IPC1)$

IPC0

DONDE:

Pr = Precio Reajustado

P = Precio Adjudicado

IPC1= Índice de Precios al consumidor publicado por el Banco Central del Paraguay, correspondiente al mes del pedido de reajuste
IPC0= Índice de Precios al Consumidor publicado por el Banco Central del Paraguay, correspondiente al mes de Apertura de Ofertas.

No se reconocerán reajuste de precios si el suministro se encuentra atrasado respecto al cronograma de entrega aprobado.

Porcentaje de multas

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

0,50 %

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

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

Tasa de interés por Mora

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

0,30

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

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

Impuestos y derechos

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

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

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

Sin excepción.

Convenios Modificatorios

La Contratante podrá acordar modificaciones al contrato conforme al artículo N° 63 de la Ley N° 2051/2003.

1. Cuando el sistema de adjudicación adoptado sea de abastecimiento simultáneo las ampliaciones de los contratos se registrarán por las disposiciones contenidas en la Ley N° 2051/2003, sus modificaciones y reglamentaciones, que para el efecto emita la DNCP.
2. Tratándose de contratos abiertos, las modificaciones a ser introducidas se registrarán atendiendo a la reglamentación vigente.
3. La celebración de un convenio modificatorio conforme a las reglas establecidas en el artículo N° 63 de la Ley 2051/2003, que constituyan condiciones de agravación del riesgo cuando la Garantía de Cumplimiento de Contrato sea formalizada a través de póliza de caución, obliga al proveedor a informar a la compañía aseguradora sobre las modificaciones a ser realizadas y en su caso, presentar ante la contratante los endosos por ajustes que se realicen a la póliza original en razón al convenio celebrado con la contratante.

Limitación de responsabilidad

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

Responsabilidad del proveedor

El proveedor deberá suministrar todos los bienes o servicios de acuerdo con las condiciones establecidas en el pliego de bases y condiciones.

Fuerza mayor

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

1. Para fines de esta cláusula, "Fuerza Mayor" significa un evento o situación fuera del control del proveedor que es imprevisible, inevitable y no se origina por

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

Causales de terminación del contrato

1. Terminación por Incumplimiento

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

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

2. Terminación por Insolvencia o quiebra

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

3. Terminación por conveniencia

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

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

- i. Que se complete alguna porción y se entregue de acuerdo con las condiciones y precios del contrato; y/o
- ii. Que se cancele la entrega restante y se pague al proveedor una suma convenida por aquellos bienes que hubiesen sido parcialmente completados y por los materiales y repuestos adquiridos previamente por el proveedor.

Otras causales de terminación del contrato

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

No Aplica

Resolución de Conflictos a través del Arbitraje

Las partes se someterán a Arbitraje:

No

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

"Todas las controversias que deriven del presente contrato o que guarden relación con éste serán resueltas definitivamente por arbitraje, conforme con las disposiciones de la ley N° 2051/03 "De Contrataciones Públicas", de la ley N° 1879/02 "De arbitraje y mediación" y las condiciones del Contrato. El procedimiento arbitral se llevará a cabo ante el Centro de Arbitraje y Mediación del Paraguay (en adelante, "CAMP"). El tribunal estará conformado por tres árbitros designados de la lista del cuerpo arbitral del CAMP, que decidirá conforme a derecho, siendo el laudo definitivo y vinculante para las partes. Se aplicará el reglamento respectivo y demás disposiciones que regule dicho procedimiento al momento de ser requerido, declarando las partes conocer y aceptar los vigentes, incluso en orden a su régimen de gastos y costas, considerándolos parte integrante del presente Contrato. Para la ejecución del laudo arbitral, o para dirimir cuestiones que no sean arbitrables, las partes se someterán a la jurisdicción de los tribunales de la ciudad de Asunción, República del Paraguay".

Fraude y Corrupción

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

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

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

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

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

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

Fraude y corrupción comprenden actos como:

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

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

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

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

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

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

MODELO DE CONTRATO

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

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

FORMULARIOS

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

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

