

PLIEGO DE BASES Y CONDICIONES

Convocante:

**Secretaria de la Funcion Publica (SFP) / Presidencia de la
República
Secretaria de la Funcion Publica**

Nombre de la Licitación:

ADQUISICIÓN DE LICENCIAS VARIAS
(versión 1)

ID de Licitación:

436060



Modalidad:

Contratación Directa

Publicado el:

11/10/2023

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

RESUMEN DEL LLAMADO

Datos de la Convocatoria

ID de Licitación:	436060	Nombre de la Licitación:	Adquisición de licencias varias
Convocante:	Secretaria de la Funcion Publica (SFP) / Presidencia de la República	Categoría:	24 - Equipos, accesorios y programas computacionales, de oficina, educativos, de imprenta, de comunicación y señalamiento
Unidad de Contratación:	Secretaria de la Funcion Publica	Tipo de Procedimiento:	CD - Contratación Directa

Etapas y Plazos

Lugar para Realizar Consultas:	Consultas virtuales a través del portal del SICP	Fecha Límite de Consultas:	13/10/2023 10:00
Lugar de Entrega de Ofertas:	Iturbe 823 esq. Fulgencio R. Moreno. DGAF 2do Piso	Fecha de Entrega de Ofertas:	18/10/2023 09:00
Lugar de Apertura de Ofertas:	Iturbe 823 esq. Fulgencio R. Moreno. DGAF 2do Piso	Fecha de Apertura de Ofertas:	18/10/2023 09:30

Adjudicación y Contrato

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

Datos del Contacto

Nombre:	Nilda E. Duarte de Godoy	Cargo:	Directora
Teléfono:	021 443 867	Correo Electrónico:	uoc@sfp.gov.py

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 esta carta de invitación, 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 de la carta de invitación 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 de la carta de invitación 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

La carta de invitación, 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 de la presente carta de invitación.

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 a la carta de invitación, 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 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:

Si para todos los ítems

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:

90

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. La garantía de mantenimiento de oferta para la presente contratación directa será expedida en formato de declaración jurada, la cual deberá estar de acuerdo con el formulario de Garantía de Mantenimiento de oferta incluido en la Sección "Formularios".
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. 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.
4. 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 la carta de invitación 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 comprobare 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.
5. En los procesos de contratación directa, la garantía de fiel cumplimiento de contrato podrá ser otorgada por medio de declaración jurada en lugar de póliza de seguro o garantía bancaria, según lo indique la Convocante en las bases de la contratación.
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:

120

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

Forma de instrumentación de la garantía de fiel cumplimiento

La garantía de cumplimiento de contrato para la presente contratación será:

Declaración Jurada

En caso de admitir la presentación de declaración jurada, el oferente deberá adecuarse al formato estándar de la Sección "Formularios".

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:

hasta el 31/01/2024

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:

48 horas hábiles, contados a partir de la notificación al proveedor del hecho de falla del equipo.

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 declaración jurada de acuerdo con el formulario de Garantía de Mantenimiento de oferta incluido en la Sección "Formularios".
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.
<ol style="list-style-type: none"> 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. (*)
<ol style="list-style-type: none"> 2. Original o fotocopia del consorcio constituido o del acuerdo de intención de constituir el consorcio por escritura pública en caso de resultar adjudicados y antes de la firma del contrato. Las formalidades de los acuerdos de intención y de los consorcios serán determinadas por la Dirección Nacional de Contrataciones Públicas (DNCP). (*)

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

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

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

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

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, en los tres últimos años (2020-2021-2022)

b. Endeudamiento: pasivo total / activo total

No deberá ser mayor a 0,80 en promedio, en los tres últimos años (2020-2021-2022)

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

El promedio en los dos tres últimos años (2020-2021-2022), no deberá ser negativo.

b) Ejemplo para contribuyentes de IRPC

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales requeridos.

c) Ejemplo para contribuyentes de IRP

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales requeridos.

d) Ejemplo de contribuyentes de exclusivamente IVA General

Deberá cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Requisitos documentales para la evaluación de la capacidad financiera

a. *Copia del Balance General y Estado de Resultados de los años (2020-2021-2022)*

b. IVA General de los últimos [3] meses, para contribuyentes sólo del IVA General

c. Formulario 106 de los últimos [3] años para contribuyentes del IRPC

d, Formulario 104 de los últimos [3] años para contribuyentes de Renta Personal.

Experiencia requerida

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

Demostrar la experiencia en la provisión de licencias y equipos informáticos similares a lo requerido en la presente convocatoria con contratos, facturaciones de venta y/o recepciones finales por un monto equivalente al 50 % como mínimo del monto total ofertado en la presente licitación de los últimos tres años. 2020-2021-2022.

Currículum de la empresa que justifique su experiencia en la provisión de licencias varias y/o equipos informáticos con un mínimo de 3 (tres) años, con un listado de clientes

Requisitos documentales para la evaluación de la experiencia

1. *Copia de contratos, facturaciones y/o recepciones finales que avalen la experiencia requerida de los años 2020-2021-2022..*

2. *Currículo de la empresa y listado de clientes*

3. *[Agregar otros documentos]*

Capacidad Técnica

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

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

- a. Declaración Jurada en la que el oferente manifiesta cuenta con lo necesario para el cumplimiento de las especificaciones técnicas requeridas.
- b. El Oferente deberá demostrar que cuenta con la Autorización Oficial, para la provisión de las licencias

Requisito documental para evaluar la capacidad técnica

1. <i>Declaración jurada de contar con lo necesario para el cumplimiento de la EETT</i>
2. Certificado de autorización del fabricante
3.

Criterios de desempate de ofertas

En caso de que existan dos o más oferentes solventes que cumplan con todos los requisitos establecidos en la carta de invitación 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 regirá de conformidad a la cláusula de adendas y cambios.

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

Identificación de la unidad solicitante y justificaciones

- *Nilda E. Duarte de Godoy, Directora de la Dirección Operativa de Contrataciones.*
- *Se solicita la adquisición y renovación de licencias varias de la SFP, los cuales soportan los programas informáticos de los sistemas administrados por este Viceministerio, como así también equipos informáticos que son necesarios para ampliar la capacidad de los equipos disponibles.*
- *La planificación se realiza de forma anual conforme a lo previsto en el Programa Anual de Contrataciones (PAC), atendiendo a los vencimientos de los certificados y licencias y la disponibilidad presupuestaria de la Institución para el Rubro 579- Activos Intangibles*
- *Las especificaciones técnicas fueron elaboradas por la Dirección General Tecnología de la Información y Comunicación, conforme a las actualizaciones y renovaciones de las licencias requeridas y los estándares para los demás equipos.*

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:

Resumen de las Especificaciones Técnicas. Los bienes deberán cumplir con las siguientes Especificaciones Técnicas y

Normas:

No. De Artículo	Nombre de los Bienes o Servicios	Especificaciones Técnicas y Normas
1	Licencia Fortigate 100 E	<i>Renovación de Licencia Fortigate 100E con periodo de actualización de 1 año desde su activación.</i>
2	Licencia Fortigate 90 E	<i>Renovación de Licencia Fortigate 90E con periodo de actualización de 1 año desde su activación.</i>
3	Licencia Red Hat Enterprise	Renovación de Red Hat Enterprise Linux Server (Physical or Virtual Nodes) Suscripción Premium por 1 año para servidores de hasta 2 sockets a partir de la fecha de finalización del soporte actual.
4	Licencia Antivirus Bif defender	Renovación de Licencia Antivirus Bif defender para 150 máquinas con periodo de actualización de 1 año desde su activación.

Ítem 1: Licencia Fortigate 100 E

Serie del Equipo Fortinet 1: FG100E4Q17005280

Serie del Equipo Fortinet 2: FG100E4Q17021564

Throughput de por lo menos 7 Gbps con la funcionalidad de firewall habilitada para tráfico IPv4 y IPv6, independiente del tamaño del paquete

Soporte a por lo menos 2M conexiones simultaneas

Soporte a por lo menos 30K nuevas conexiones por segundo

Throughput de al menos 4 Gbps de VPN IPSec

Estar licenciado para, o soportar sin necesidad de licencia, 2K túneles de VPN IPSec site-to-site simultáneos

Estar licenciado para, o soportar sin necesidad de licencia, 10K túneles de clientes VPN IPSec simultáneos

Throughput de al menos 250 Mbps de VPN SSL

Soportar al menos 300 clientes de VPN SSL simultáneos

Soportar al menos 500 Gbps de throughput de IPS

Soportar al menos 190 Mbps de throughput de Inspección SSL

Throughput de al menos 250 Mbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la solución de seguridad tenga debidamente activadas y operativas: control de aplicaciones, IPS, Antivirus y Antispyware. Caso el fabricante tenga publicado múltiples números de desempeño para cualquiera de las funcionalidades, solamente el de valor más pequeño será aceptado.

Permitir gestionar al menos 32 Access Points

Tener al menos 14 interfaces 1Gbps

Estar licenciado y/o tener incluido sin costo adicional, al menos 10 sistemas virtuales lógicos (Contextos) por appliance

Soporte a por lo menos 10 sistemas virtuales lógicos (Contextos) por appliance

La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.;

Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;

Las funcionalidades de protección de red que conforman la plataforma de seguridad, pueden ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;

La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;

Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación;

La gestión de equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red;

Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;

Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP;

Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding;

Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM);

Los dispositivos de protección de red deben soportar DHCP Relay;

Los dispositivos de protección de red deben soportar DHCP Server;

Los dispositivos de protección de red deben soportar sFlow;

Los dispositivos de protección de red deben soportar Jumbo Frames;

Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;

Debe ser compatible con NAT dinámica (varios-a-1);

Debe ser compatible con NAT dinámica (muchos-a-muchos);

Debe soportar NAT estática (1-a-1);

Debe admitir NAT estática (muchos-a-muchos);

Debe ser compatible con NAT estático bidireccional 1-a-1;

Debe ser compatible con la traducción de puertos (PAT);

Debe ser compatible con NAT Origen;

Debe ser compatible con NAT de destino;

Debe soportar NAT de origen y NAT de destino de forma simultánea;

Debe soportar NAT de origen y NAT de destino en la misma política

Debe soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico;

Debe ser compatible con NAT64 y NAT46;

Debe implementar el protocolo ECMP;

Debe soportar el balanceo de enlace hash por IP de origen;

Debe soportar el balanceo de enlace por hash de IP de origen y destino;

Debe soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces;

Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales;

Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;

Enviar logs a sistemas de gestión externos simultáneamente;

Debe tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL;

Debe soportar protección contra la suplantación de identidad (anti-spoofing);

Implementar la optimización del tráfico entre dos dispositivos;

Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);

Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);

Soportar OSPF graceful restart;

Los dispositivos de protección deben tener la capacidad de operar simultáneamente en una única instancia de servidor de seguridad, mediante el uso de sus interfaces físicas en los siguientes modos: modo sniffer (monitoreo y análisis de tráfico de red), capa 2 (L2) y capa 3 (L3);

Debe ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red;

Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;

Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;

Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;

Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente;

Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3;

Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster;

La configuración de alta disponibilidad debe sincronizar: Sesiones;

La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red;

La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN;

La configuración de alta disponibilidad debe sincronizar: Tablas FIB;

En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace;

Debe soportar la creación de sistemas virtuales en el mismo equipo;

Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos;

Debe permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales;

La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso;

Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos);

Debe soportar un tejido de seguridad para proporcionar una solución de seguridad integral que abarque toda la red;

El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red;

Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi;

Debe soportar controles de zona de seguridad;

Debe contar con políticas de control por puerto y protocolo;

Contar con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones;

Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad;

Firewall debe poder aplicar la inspección UTM (control de aplicaciones y filtrado web como mínimo) directamente a las políticas de seguridad en vez de usar perfil obligatoriamente;

Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall;

Debe soportar el almacenamiento de bitácoras (logs) en tiempo real tanto para entorno de la nube como entorno local (on-premise);

Debe soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF);

Debe existir una manera de evitar que el almacenamiento de logs en tiempo real no supere la velocidad de subida de los mismos (upload);

Debe soportar el protocolo estándar de la industria VXLAN;

Los dispositivos de protección de red deben tener la capacidad de reconocer las aplicaciones, independientemente del puerto y protocolo;

Debe ser posible liberar y bloquear aplicaciones sin necesidad de abrir o cerrar puertos y protocolos;

Reconocer al menos 1.700 aplicaciones diferentes, incluyendo, pero no limitado a: El tráfico relacionado peer-to-peer, redes sociales, acceso remoto, actualización de software, protocolos de red, VoIP, audio, vídeo, Proxy, mensajería instantánea, compartición de archivos, correo electrónico;

Reconocer al menos las siguientes aplicaciones: BitTorrent, Gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

Debe inspeccionar el payload del paquete de datos con el fin de detectar las firmas de las aplicaciones conocidas por el fabricante independiente de puerto y protocolo;

Debe detectar aplicaciones a través del análisis del comportamiento del tráfico observado, incluyendo, pero no limitado a las aplicaciones de VoIP que utilizan cifrado propietario y BitTorrent;

Identificar el uso de tácticas evasivas, es decir, debe tener la capacidad de ver y controlar las aplicaciones y los ataques con tácticas evasivas a través de las comunicaciones cifradas, tales como Skype y la utilización de la red Tor;

Para tráfico cifrado SSL, debe poder descifrarlo a fin de posibilitar la lectura de payload para permitir la identificación de firmas de la aplicación conocidas por el fabricante;

Debe hacer decodificación de protocolos con el fin de detectar aplicaciones encapsuladas dentro del protocolo y validar que el tráfico corresponde a la especificación del protocolo, incluyendo, pero no limitado a Yahoo Instant Messenger utilizando HTTP. La decodificación de protocolo también debe identificar las características específicas dentro de una aplicación, incluyendo, pero no limitado al intercambio de ficheros dentro de Webex;

Identificar el uso de tácticas evasivas a través de las comunicaciones cifradas;

Actualización de la base de firmas de la aplicación de forma automática;

Limitar el ancho de banda (carga / descarga) utilizado por las aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos;

Los dispositivos de protección de red deben tener la capacidad de identificar al usuario de la red con la integración de Microsoft Active Directory sin necesidad de instalación del agente en el controlador de dominio, o en estaciones de trabajo de usuario;

Debe ser posible añadir múltiples reglas de control de aplicaciones, es decir, no debe limitar habilitar el control de aplicaciones de control solamente en algunas reglas;

Debe ser compatible con múltiples métodos de identificación y clasificación de las aplicaciones, al menos verificar firmas y protocolos de decodificación;

Para mantener la seguridad de red eficiente debe soportar el control de las aplicaciones desconocidas y no sólo en aplicaciones conocidas;

Permitir la creación de forma nativa de firmas personalizadas para el reconocimiento de aplicaciones propietarias en su propia interfaz gráfica, sin la necesidad de la acción del fabricante;

La creación de firmas personalizadas debe permitir el uso de expresiones regulares, el contexto (sesiones o transacciones), utilizando la posición en el payload de paquetes TCP y UDP, y el uso de decodificadores de al menos los siguientes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, SSL y RTSP;

El fabricante debe permitir solicitar la inclusión de aplicaciones en su base de datos;

Debe alertar al usuario cuando sea bloqueada una aplicación;

Debe permitir la diferenciación de tráfico Peer2Peer (Bittorrent, eMule, etc) permitiendo granularidad de control/reglas para el mismo;

Debe permitir la diferenciación de tráfico de mensajería instantánea (AIM, Hangouts, Facebook Chat, etc.) permitiendo granularidad de control/reglas para el mismo;

Debe permitir la diferenciación y manejo de las aplicaciones de chat; por ejemplo permitir a Hangouts el chat pero impedir la llamada de video;

Debe permitir la diferenciación de aplicaciones Proxies (psiphon, Freegate, etc.) permitiendo granularidad de control/reglas para el mismo;

Debe ser posible la creación de grupos dinámicos de aplicaciones, basado en las características de las mismas, tales como: Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc);

Debe ser posible crear grupos dinámicos de aplicaciones basados en características de las mismas, tales como: Nivel de riesgo de la aplicación;

Debe ser posible crear grupos estáticos de aplicaciones basadas en características de las mismas, tales como: Categoría de Aplicación;

Debe ser posible configurar Application Override seleccionando las aplicaciones individualmente

Para proteger el entorno contra los ataques, deben tener módulo IPS, antivirus y anti-spyware integrado en el propio equipo;

Debe incluir firmas de prevención de intrusiones (IPS) y el bloqueo de archivos maliciosos (antivirus y anti-spyware);

Las características de IPS, antivirus y anti-spyware deben funcionar de forma permanente, pudiendo utilizarlas de forma indefinida, aunque no exista el derecho a recibir actualizaciones o no exista un contrato de garantía del software con el fabricante;

Debe sincronizar las firmas de IPS, antivirus, anti-spyware cuando se implementa en alta disponibilidad;

Debe implementar los siguientes tipos de acciones a las amenazas detectadas por IPS: Permitir, permitir y generar registro, bloquear, bloquear IP del atacante durante un tiempo y enviar tcp-reset;

Las firmas deben ser capaces de ser activadas o desactivadas, o activadas sólo en el modo de monitoreo;

Debe ser posible crear políticas para usuarios, grupos de usuarios, IP, redes o zonas de seguridad;

Excepciones por IP de origen o destino deben ser posibles en las reglas o en cada una de las firmas;

Debe soportar granularidad en las políticas de IPS, Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos estos elementos;

Deber permitir el bloqueo de vulnerabilidades;

Debe permitir el bloqueo de exploits conocidos;

Debe incluir la protección contra ataques de denegación de servicio;

Debe tener los siguientes mecanismos de inspección IPS: Análisis de patrones de estado de las conexiones;

Debe tener los siguientes mecanismos de inspección IPS: Análisis de decodificación de protocolo;

Debe tener los siguientes mecanismos de inspección IPS: Análisis para detectar anomalías de protocolo;

Debe tener los siguientes mecanismos de inspección IPS: Análisis heurístico;

Debe tener los siguientes mecanismos de inspección IPS: Desfragmentación IP;

Debe tener los siguientes mecanismos de inspección IPS: Re ensamblado de paquetes TCP;

Debe tener los siguientes mecanismos de inspección IPS: Bloqueo de paquetes con formato incorrecto (malformed packets);

Debe ser inmune y capaz de prevenir los ataques básicos, tales como inundaciones (flood) de SYN, ICMP, UDP, etc;

Detectar y bloquear los escaneos de puertos de origen;

Bloquear ataques realizados por gusanos (worms) conocidos;

Contar con firmas específicas para la mitigación de ataques DoS y DDoS;

Contar con firmas para bloquear ataques de desbordamiento de memoria intermedia (buffer overflow);

Debe poder crear firmas personalizadas en la interfaz gráfica del producto;

Debe permitir utilizar operadores de negación en la creación de firmas personalizadas de IPS o anti-spyware, permitiendo la creación de excepciones con granularidad en la configuración;

Permitir bloqueo de virus y software espía en por lo menos los siguientes protocolos: HTTP, FTP, SMB, SMTP y POP3;

Soportar el bloqueo de archivos por tipo;

Identificar y bloquear la comunicación con redes de bots;

Registrar en la consola de supervisión la siguiente información sobre amenazas concretas: El nombre de la firma o el ataque, la aplicación, el usuario, el origen y destino de las comunicaciones, además de las medidas adoptadas por el dispositivo;

Debe ser compatible con la captura de paquetes (PCAP), mediante la firma de IPS o control de aplicación;

Debe permitir la captura de paquetes por tipo de firma IPS y definir el número de paquetes capturados o permitir la captura del paquete que dio lugar a la alerta, así como su contexto, facilitando el análisis forense y la identificación de falsos positivos;

Debe tener la función de protección a través de la resolución de direcciones DNS, la identificación de nombres de resolución de las solicitudes a los dominios maliciosos de botnets conocidos;

Los eventos deben identificar el país que origino la amenaza;

Debe incluir protección contra virus en contenido HTML y Javascript, software espía (spyware) y gusanos (worms);

Tener protección contra descargas involuntarias mediante archivos ejecutables maliciosos y HTTP;

Debe permitir la configuración de diferentes políticas de control de amenazas y ataques basados en políticas de firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc., es decir, cada política de firewall puede tener una configuración diferente de IPS basada en usuario, grupos de usuarios, origen, destino, zonas de seguridad;

El Firewall debería permitirle analizar la implementación del tejido de seguridad para identificar posibles vulnerabilidades y resaltar las mejores prácticas que podrían utilizarse para mejorar la seguridad y el rendimiento general de su red;

En caso de que el firewall pueda coordinarse con software de seguridad en equipo de usuario final (LapTop, DeskTop, etc) deberá contar con un perfil donde pueda realizar análisis de vulnerabilidad en estos equipos de usuario y asegurarse de que estos ejecuten versiones compatibles;

Los recursos de postura de seguridad deben existir para permitir que el software de seguridad de endpoint aplique protección en tiempo real, antivirus, filtrado de Web y control de aplicaciones en el punto final;

Proporcionan protección contra ataques de día cero a través de una estrecha integración con componentes del tejido de seguridad, incluyendo NGFW y Sandbox (en las instalaciones y en la nube);

Debe permitir especificar la política por tiempo, es decir, la definición de reglas para un tiempo o período determinado (día, mes, año, día de la semana y hora);

Debe ser posible crear políticas para usuarios, IPs, redes, o zonas de seguridad;

Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está utilizando las URL esto mediante la integración con los servicios de directorio Active Directory y la base de datos local;

Debe tener la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando las URL que mediante la integración con los servicios de directorio Active Directory y la base de datos local, en modo de proxy transparente y explícito;

Debe soportar la capacidad de crear políticas basadas en control por URL y categoría de URL;

Debe tener la base de datos de URLs en caché en el equipo o en la nube del fabricante, evitando retrasos de comunicación / validación de direcciones URL;

Tener por lo menos 60 categorías de URL;

Debe tener la funcionalidad de exclusión de URLs por categoría;

Permitir página de bloqueo personalizada;

Permitir bloqueo y continuación (que permita al usuario acceder a un sitio potencialmente bloqueado, informándole en pantalla del bloqueo y permitiendo el uso de un botón Continuar para que el usuario pueda seguir teniendo acceso al sitio);

Además del Explicit Web Proxy, soportar proxy web transparente;

Se debe incluir la capacidad de crear políticas basadas en la visibilidad y el control de quién está usando dichas aplicaciones a través de la integración con los servicios de directorio, a través de la autenticación LDAP, Active Directory, E-diretorio y base de datos local;

Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos, permitiendo granularidad a las políticas / control basados en usuarios y grupos de usuarios;

Debe tener integración y soporte para Microsoft Active Directory para los siguientes sistemas operativos: Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 y Windows Server 2012 R2;

Debe tener integración con Microsoft Active Directory para identificar a los usuarios y grupos que permita tener granularidad en las políticas/control basados en usuarios y grupos de usuarios, soporte a single-sign-on. Esta funcionalidad no debe tener límites licenciados de usuarios o cualquier restricción de uso como, pero no limitado a, utilización de sistemas virtuales, segmentos de red, etc;

Debe tener integración con RADIUS para identificar a los usuarios y grupos que permiten las políticas de granularidad / control basados en usuarios y grupos de usuarios;

Debe tener la integración LDAP para la identificación de los usuarios y grupos que permiten granularidad en la política/control basados en usuarios y grupos de usuarios;

Debe permitir el control sin necesidad de instalación de software de cliente, el equipo que solicita salida a Internet, antes de iniciar la navegación, entre a un portal de autenticación residente en el equipo de seguridad (portal cautivo);

Debe soportar la identificación de varios usuarios conectados a la misma dirección IP en entornos Citrix y Microsoft Terminal Server, lo que permite una visibilidad y un control granular por usuario en el uso de las aplicaciones que se encuentran en estos servicios;

Debe de implementar la creación de grupos de usuarios en el firewall, basada atributos de LDAP / AD;

Permitir la integración con tokens para la autenticación de usuarios, incluyendo, pero no limitado a, acceso a Internet y gestión de la plataforma;

Proporcionar al menos un token de forma nativa, lo que permite la autenticación de dos factores;

Con el fin de controlar el tráfico y aplicaciones cuyo consumo puede ser excesivo (como YouTube, Ustream, etc.) y que tienen un alto consumo de ancho de banda, se requiere de la solución que, además de permitir o denegar dichas solicitudes, debe tener la capacidad de controlar el ancho de banda máximo cuando son solicitados por los diferentes usuarios o aplicaciones, tanto de audio como de video streaming;

Soportar la creación de políticas de QoS y Traffic Shaping por dirección de origen;

Soportar la creación de políticas de QoS y Traffic Shaping por dirección de destino;

Soportar la creación de políticas de QoS y Traffic Shaping por usuario y grupo;

Soportar la creación de políticas de QoS y Traffic Shaping para aplicaciones incluyendo, pero no limitado a Skype, BitTorrent, Azureus y YouTube;

Soportar la creación de políticas de calidad de servicio y Traffic Shaping por puerto;

En QoS debe permitir la definición de tráfico con ancho de banda garantizado;

En QoS debe permitir la definición de tráfico con máximo ancho de banda;

En QoS debe permitir la definición de colas de prioridad;

Soportar la priorización de protocolo en tiempo real de voz (VoIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype;

Soportar marcación de paquetes DiffServ, incluso por aplicación;

Soportar la modificación de los valores de DSCP para Diffserv;

Soportar priorización de tráfico utilizando información de Tipo de Servicio (Type of Service);

Proporcionar estadísticas en tiempo real para clases de QoS y Traffic Shaping;

Debe soportar QoS (traffic-shapping) en las interfaces agregadas o redundantes;

Permite la creación de filtros para archivos y datos predefinidos;

Los archivos deben ser identificados por tamaño y tipo;

Permitir identificar y opcionalmente prevenir la transferencia de varios tipos de archivo (MS Office, PDF, etc.) identificados en las aplicaciones (HTTP, FTP, SMTP, etc.);

Soportar la identificación de archivos comprimidos o la aplicación de políticas sobre el contenido de este tipo de archivos;

Soportar la identificación de archivos cifrados y la aplicación de políticas sobre el contenido de este tipo de archivos;

Permitir identificar y opcionalmente prevenir la transferencia de información sensible, incluyendo, pero no limitado a, número de tarjeta de crédito, permitiendo la creación de nuevos tipos de datos a través de expresiones regulares;

Soportar la creación de políticas por geolocalización, permitiendo bloquear el tráfico de cierto País/Países;

Debe permitir la visualización de los países de origen y destino en los registros de acceso;

Debe permitir la creación de zonas geográficas por medio de la interfaz gráfica de usuario y la creación de políticas usando las mismas;

Soporte VPN de sitio-a-sitio y cliente-a-sitio;

Soportar VPN IPSec;

Soportar VPN SSL;

La VPN IPSec debe ser compatible con 3DES;

La VPN IPSec debe ser compatible con la autenticación MD5 y SHA-1;

La VPN IPSec debe ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14;

La VPN IPSec debe ser compatible con Internet Key Exchange (IKEv1 y v2);

La VPN IPSec debe ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard);

La VPN IPSec debe ser compatible con la autenticación a través de certificados IKE PKI;

Debe tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

Soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec;

Debe permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting;

La VPN SSL debe soportar que el usuario pueda realizar la conexión a través de cliente instalado en el sistema operativo de su máquina o a través de la interfaz web;

Las características de VPN SSL se deben cumplir con o sin el uso de agentes;

Debe permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy;

Asignación de DNS en la VPN de cliente remoto;

Debe permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL;

Suportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;

Suportar lectura y revisión de CRL (lista de revocación de certificados);

Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL;

Debe permitir que la conexión a la VPN se establezca de la siguiente manera: Antes de que el usuario se autentique en su estación;

Debe permitir que la conexión a la VPN se establezca de la siguiente manera: Después de la autenticación de usuario en la estación;

Debe permitir que la conexión a la VPN se establezca de la siguiente manera: Bajo demanda de los usuarios;

Deberá mantener una conexión segura con el portal durante la sesión;

El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows 7 (32 y 64 bits), Windows 8 (32 y 64 bits), Windows 10 (32 y 64 bits) y Mac OS X (v10.10 o superior);

Deberá gestionar de manera centralizada puntos de acceso del mismo fabricante de la solución ofertada;

Soportar servicio de servidor DHCP por SSID para proporcionar direcciones IP a los clientes inalámbricos;

Soporte IPv4 e IPv6 por SSID;

Permitir elegir si el tráfico de cada SSID se enviará a la controladora o directamente por la interfaz de punto de acceso en una determinada VLAN;

Permitir definir qué redes se acceden a través de la controladora y que redes serán accedidas directamente por la interfaz del Access Point;

Soportar monitoreo y supresión de puntos de acceso indebidos;

Proporcionar autenticación a la red inalámbrica a través de bases de datos externas, tales como LDAP o RADIUS;

Permitir autenticar a los usuarios de la red inalámbrica de manera transparente en dominios Windows;

Permitir la visualización de los dispositivos inalámbricos conectados por usuario;

Permitir la visualización de los dispositivos inalámbricos conectados por IP;

Permitir la visualización de los dispositivos inalámbricos conectados por tipo de autenticación;

Permitir la visualización de los dispositivos inalámbricos conectados por canal;

Permitir la visualización de los dispositivos inalámbricos conectados por ancho de banda usado;

Permitir la visualización de los dispositivos inalámbricos conectados por potencia de la señal;

Permitir la visualización de los dispositivos inalámbricos conectados por tiempo de asociación;

Debe soportar Fast Roaming en autenticación con portal cautivo;

Debe soportar configuración de portal cautivo por SSID;

Permitir bloqueo de tráfico entre los clientes conectados a un SSID y AP específico;

Debe ser compatible con Wi-Fi Protected Access (WPA) y WPA2 por SSID, usando un algoritmo AES y / o TKIP;

Debe ser compatible con el protocolo 802.1x RADIUS;

La controladora inalámbrica deberá permitir configurar los parámetros de radio como banda y canal;

La controladora deberá permitir métodos de descubrimiento de puntos de acceso de manera automática;

La controladora deberá permitir métodos de descubrimiento de puntos de acceso por IP estática;

La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DHCP;

La controladora deberá permitir métodos de descubrimiento de puntos de acceso por DNS;

La controladora deberá permitir métodos de descubrimiento de puntos de acceso por Broadcast;

La controladora deberá permitir métodos de descubrimiento de puntos de acceso por Multicast;

La controladora inalámbrica deberá suministrar una lista de Puntos de Acceso autorizados y puntos de acceso indebidos (Rogue);

La controladora deberá contar con protección contra ataques ARP Poisoning en el controlador inalámbrico;

La controladora deberá contar con mecanismos de protección de tramas de administración de acuerdo a las especificaciones de la alianza Wi-Fi y estándar 802.11ac;

La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo ASLEAP;

La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Association Frame Flooding;

La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Authentication Frame Flooding;

La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Broadcasting De-authentication;

La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo EAPOL Packet flooding;

La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Invalid MAC OUI;

La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Long Duration Attack;

La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Null SSID probe response;

La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Spoofed De-authentication;

La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Weak WEP IV Detection;

La controladora inalámbrica deberá tener de manera integrada sistema de detección de intrusión inalámbrica contra ataques tipo Wireless Bridge;

Implementar canales de auto-aprovisionamiento de los puntos de acceso con el fin de minimizar la interferencia entre ellas;

Permitir seleccionar el día y hora en que se producirá la optimización de aprovisionamiento automática de canales en los puntos de acceso;

La controladora inalámbrica debe permitir agendar horarios para determinar en qué momento la red inalámbrica (SSID) se encuentra disponible;

La controladora inalámbrica debe ofrecer funcionalidad de Firewall integrado UTM basado en la identidad del usuario;

Permitir configurar el número máximo de clientes que pueden ser permitidos por SSID;

Permitir configurar el número máximo de clientes que pueden ser permitidos por punto de acceso;

Permitir configurar el número máximo de clientes que pueden ser permitidos por Radio;

La controladora debe permitir crear, administrar y autorizar las redes inalámbricas mesh;

Ofrecer un mecanismo de creación automática y/o manual de usuarios visitantes y contraseñas, que puedan ser enviados por correo electrónico o SMS a los usuarios, con ajuste de tiempo de expiración de la contraseña;

La comunicación entre la controladora y el punto de acceso inalámbrico pueda ser realizada de forma cifrada utilizando protocolo DTLS;

Debe tener un mecanismo de ajuste automático de potencia de la señal con el fin de reducir la interferencia entre canales entre dos puntos de acceso administrados;

Ofrecer un mecanismo de balanceo de tráfico/usuarios entre Puntos de acceso;

Proporcionar un mecanismo de balanceo de tráfico/usuarios entre frecuencias y/o radios de los Puntos de Acceso;

Debe permitir la identificación del firmware utilizado por cada punto de acceso gestionado y permitir la actualización a través de la interfaz gráfica;

Permitir que sean deshabilitados clientes inalámbricos que tengan baja tasa de transmisión;

Permitir ignorar a los clientes inalámbricos que tienen señal débil, estableciendo un umbral de señal a partir de la cual los clientes son ignorados;

La controladora debe permitir configurar el valor de Short Guard Interval para 802.11n y 802.11ac en 5 GHz;

Debe permitir seleccionar individualmente para cada punto de acceso los SSID que van a ser propagados;

Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID específico mediante protocolo RADIUS;

Debe permitir asociación dinámica de VLANs a los usuarios autenticados en un SSID específico mediante vlan pooling;

Debe permitir visualizar las aplicaciones y amenazas por cada dispositivo inalámbrico;

La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en aplicaciones;

La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en dirección de destino;

La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en amenaza;

La controladora inalámbrica debe permitir identificar los clientes WiFi que presenten algún riesgo basado en sesiones;

la controladora inalámbrica debe soportar una licencia que permita al menos 10000 firmas de aplicaciones para reconocimiento de tráfico;

El controlador inalámbrico debe tener interfaz de administración integrado en el mismo equipo;

El controlador inalámbrico debe soportar la funcionalidad de Fast-roaming para enlaces mesh entre el nodo secundario y nodos principales;

La controladora inalámbrica deberá soportar aceleración de tráfico del protocolo CAPWAP a través de un procesador de red de propósito específico;

La controladora inalámbrica deberá soportar aceleración de túnel de tráfico de puente inalámbrico a través de un procesador de red de propósito específico;

La controladora inalámbrica debe soportar protocolo LLDP;

Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC exacta;

Debe permitir técnica de detección de APs intrusos On-wire a través de dirección MAC adyacente;

Debe permitir la visualización de los usuarios conectados en forma de topología lógica de red representando la cantidad de datos transmitidos y recibidos;

La controladora inalámbrica debe permitir combinar redes WiFi y redes cableadas con un software switch integrado;

La controladora inalámbrica debe permitir crear un portal cautivo en el software switch integrado para redes WiFi y redes cableadas;

La controladora inalámbrica debe permitir gestionar switches de acceso del mismo fabricante de la solución ofertada;

Deberá soportar la conversión de Multicast a Unicast para mejorar el rendimiento del tiempo de aire;

En el entorno de alta disponibilidad, debe existir el concepto de controladores primarios y secundarios en la unidad AP, permitiendo que la unidad decida el orden en el que el AP selecciona una unidad controlador y cómo la unidad AP se conecta a un controlador de backup en el caso de que el controlador primario falle;

Debe proporcionar la capacidad de crear varias claves pre-compartidas de acceso protegido WiFi (WPA-PSK) para que no sea necesario compartir PSK entre dispositivos;

Ítem 2: Licencia Fortigate 90 E

Especificaciones Técnicas para renovación de licencia Fortigate Router 90E

Serie del Equipo Fortinet: FGT90E4Q16000910

Puertos GE RJ45	16
Puertos USB	1
Puerto Consola (RJ45)	1
Rendimiento del Firewall	4.0 Gbps
Latencia del Firewall (64 byte UDP Packets)	182 µs
Rendimiento Firewall (PPS)	375 Kpps
Sesiones Concurrentes (TCP)	1.2 Millón
Sesiones Nuevas/Sec (TCP)	27,500
Políticas de Firewall	5,000
Rendimiento de IPSec VPN (512 byte)	160 Mbps
Gateway a Gateway IPSec VPN Tunnels	200
Cliente a Gateway IPSec VPN Tunnels	2,500
Rendimiento del SSL-VPN	95 Mbps
Usuarios Concurrentes SSL-VPN	200
(Máximo Recomendado)	
Rendimiento del IPS (HTTP / Enterprise Mix)	950 / 440 Mbps
Rendimiento del SSL Inspection	300 Mbps
Rendimiento del Application Control	450 Mbps
Rendimiento NGFW	350 Mbps
Rendimiento Threat Protection	210 Mbps
Rendimiento CAPWAP	2.2 Gbps
Virtual Domains (Default / Máximo)	10 / 10
Configuraciones de alta disponibilidad	Activo / Activo, Activo / Pasivo, Clustering

Requerimiento de Energía	100240V AC, 6050 Hz
(Adaptador Externo de Energía)	
Corriente máxima	240V AC / 0.75A
Consumo de energía (promedio / máximo)	23.7 W / 28.44 W
Calor Disipado	80.8644 BTU/h
Temperatura de Operación	040°C
Temperatura de Almacenamiento	-3570°C
Humedad	2090% Sin Condensación
Nivel de Ruido	38.8 at 25°C @ 1m (Máximo: 40 dB at 25°C)
Certificación y Cumplimiento	FCC Part 15 Class B, C-Tick, VCCI, CE, UL/cUL, ICSA Labs:
Firewall, IPSec, IPS, Antivirus,SSL VPN; USGv6/IPv6 UL/cUL, CB	

Ítem 3: Licencias Red Hat Enterprise Linux Server

N°	Descripción
1	Renovación de Red Hat Enterprise Linux Server (Physical or Virtual Nodes) Suscripción Premium por 1 año para servidores de hasta 2 sockets.
2	Ampliación de Red Hat Enterprise Linux Server (Physical or Virtual Nodes) Suscripción Premium por 1 año para servidores de hasta 2 sockets.

Características

- Fácil de administrar y controlar aplicaciones en hardware físico, máquinas virtuales y la nube.
- Alto grado de escalabilidad y rendimiento
- Sistema de archivos predeterminado altamente escalable, sólido y flexible
- Arquitectura adaptable a ambientes heterogéneos
- Posee tecnologías de seguridad y certificación para implementación en agencias de gobierno
- Posee funciones de fiabilidad, disponibilidad y facilidad de servicio
- Garantiza la disponibilidad y la integridad de los datos en el sistema de archivos de clusters
- Entorno flexible para realizar el traslado desde entornos físicos a virtuales o de nube

Observación: los proveedores deben contar con soporte local y poseer los certificados proveídos por el fabricante.

Ítem 4: Licencia Antivirus Bit defender

Nro.	Descripción
1	Renovación de Licencia Antivirus Bif defender para 150 máquinas con periodo de actualización de 1 año desde su activación.

Descripción

- Actualización en línea bases de datos de virus durante todo el periodo de licenciamiento.
- Antimalware en tiempo-real escaneado basado en firmas, proactivo.
- Controles de puntos finales (de aplicaciones, de dispositivos y web)

- Análisis automático de vulnerabilidades y distribución de parches
- Firewall
- Análisis heurístico
- Protección asistida en la nube
- Control de dispositivos extraíbles (Posibilidad de poder bloquear dichos dispositivos)
- Antivirus para el correo
- Antivirus para chat
- Prevención de intrusos
- Prevención de exploit
- Lista blanca de aplicaciones
- Escáner de vulnerabilidades avanzado
- Acceso a nuevas versiones de productos
- Soporte Estándar permanente sin costo. Este incluye: Soporte telefónico, remoto y por correo/ticket, de lunes a viernes de 8:00 a 18:00 hs.
- Soporte por parte del fabricante
- Kit de administración centralizada (Security center)
- Certificado de autenticidad del producto.
- Disponer de una única consola de administración centralizada que permitan visualizar globalmente, de una manera resumida y en tiempo real.
- Herramientas de administración de sistemas fáciles de usar

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:

Ítem	Descripción del bien	Cantidad	Unidad de medida	Lugar de entrega de los bienes	Fecha(s) final(es) de entrega de los bienes
1	Licencia Fortigate 100 E	2	unidad	Viceministerio de Capital Humano y Gestión Organizacional	10 días hábiles contados a partir de la emisión de la orden de compra correspondiente
2	Licencia Fortigate 90 E	1	unidad	Viceministerio de Capital Humano y Gestión Organizacional	10 días hábiles contados a partir de la emisión de la orden de compra correspondiente
3	Licencia Red Hat Enterprise	2	unidad	Viceministerio de Capital Humano y Gestión Organizacional	10 días hábiles contados a partir de la emisión de la orden de compra correspondiente

4	Licencia Antivirus Bif defender	150	unidad	Viceministerio de Capital Humano y Gestión Organizacional	10 días hábiles contados a partir de la emisión de la orden de compra correspondiente
---	---------------------------------	-----	--------	---	---

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))
	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA

Planos y diseños

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

No Aplica

Embalajes y documentos

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

No Aplica

Inspecciones y pruebas

Las inspecciones y pruebas serán como se 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
Acta de recepción de Licencia Fortinet de 100 E	Acta	Diciembre/2023
Acta de recepción de Licencia Fortigate 90 E	Acta	Diciembre/2023
Acta de recepción de Licencia Red Hat Enterprise	Acta	Diciembre/2023
Acta de recepción de Licencia Antivirus Bif defender	Acta	Diciembre/2023

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 la carta de invitación, 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
<ul style="list-style-type: none">• Certificado de no encontrarse en quiebra o en convocatoria de acreedores expedido por la Dirección General de Registros Públicos;
<ul style="list-style-type: none">• Certificado de no hallarse en interdicción judicial expedido por la Dirección General de Registros Públicos;
<ul style="list-style-type: none">• Constancia de no adeudar aporte obrero patronal expedida por el Instituto de Previsión Social.
<ul style="list-style-type: none">• 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
<ul style="list-style-type: none">• 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.
<ul style="list-style-type: none">• Certificado de cumplimiento tributario vigente a la firma del contrato.
2. Documentos. Consorcios
<ul style="list-style-type: none">• Cada integrante del Consorcio que sea una persona física o jurídica deberá presentar los documentos requeridos para oferentes individuales especificados en los apartados precedentes.
<ul style="list-style-type: none">• Original o fotocopia del Consorcio constituido
<ul style="list-style-type: none">• Documentos que acrediten las facultades del firmante del contrato para comprometer solidariamente al consorcio.
<ul style="list-style-type: none">• 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: Se solicitará el pago por medio de una nota dirigida a la Secretaría de la Función adjuntando los documentos citados anteriormente

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 precio del contrato estará sujeto a reajustes. La fórmula y el procedimiento para el reajuste serán los siguientes: La siguiente fórmula será aplicada para los productos de origen nacional cuando la variación del Índice de Precios de Consumo (IPC) publicado por el BCP haya sufrido una variación igual o mayor al quince por ciento (15%) referente a la fecha de apertura de ofertas según lo establecido en el art. 61 de la Ley 2051/03

$$Pr = P \times IPC1 / IPC0$$

Donde:

Pr: Precio Reajustado.

P: Precio adjudicado

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

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

No se reconocerán reajustes de precios si el suministro se encuentra atrasado respecto al cronograma de entregas 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:

0,10 %

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:

0,01

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

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

Impuestos y derechos

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

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

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

No Aplica

Convenios Modificatorios

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

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

Limitación de responsabilidad

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

Responsabilidad del proveedor

El proveedor deberá suministrar todos los bienes o servicios de acuerdo con las condiciones establecidas en la carta de invitación.

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).

Formalización de la Contratación

La convocante formalizará la contratación mediante:

CONTRATO

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.

