REPÚBLICA DEL PARAGUAY

PLIEGO DE BASES Y CONDICIONES

Convocante:

Corte Suprema de Justicia (CSJ)

Corte Suprema de Justicia

Nombre de la Licitación:

ADQUISICION DE SWITCHES DE RED (CORE, ACCESO Y DATA CENTER) PARA LA DIRECCIÓN GENERAL DE LOS REGISTROS PUBLICOS - PLURIANUAL - AD REFERENDUM - S.B.E

(versión 2)

ID de Licitación:

436636

Modalidad:

Licitación Pública Nacional

Publicado el:

09/04/2024

RESUMEN DEL LLAMADO

Datos de la Convocatoria

ID de Licitación:	436636	**Nombre de la Licitación:**	ADQUISICION DE SWITCHES DE RED (CORE, ACCESO Y DATA CENTER) PARA LA DIRECCIÓN GENERAL DE LOS REGISTROS PUBLICOS - PLURIANUAL - AD REFERENDUM - S.B.E
Convocante:	Corte Suprema de Justicia (CSJ)	**Categoría:**	24 - Equipos, accesorios y programas computacionales, de oficina, educativos, de imprenta, de comunicación y señalamiento
Unidad de Contratación:	Corte Suprema de Justicia	**Tipo de Procedimiento:**	LPN - Licitación Pública Nacional

Etapas y Plazos

Lugar para Realizar Consultas:	Consultas Virtuales a traves del portal	**Fecha Límite de Consultas:**	03/04/2024 10:00
Lugar de Entrega de Ofertas:	Alonso y Testanova - Palacio de Justicia - 4to piso Torre Sur - UOC	**Fecha de Entrega de Ofertas:**	26/04/2024 09:15
Lugar de Apertura de Ofertas:	Alonso y Testanova - Palacio de Justicia - 4to piso Torre Sur - UOC	**Fecha de Apertura de Ofertas:**	26/04/2024 09:30

Adjudicación y Contrato

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

Datos del Contacto

Nombre:	Lic. Liz Fátima Insfrán	**Cargo:**	Directora
Teléfono:	424460	**Correo Electrónico:**	CONTRATACIONES1@PJ.GOV.PY

ADENDA

Adenda

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

ADENDA N° 1

Por la que se introducen modificaciones o enmiendas en el SICP.

Se modifican los siguientes eventos:

*Fecha Tope de Respuesta

*Fecha Inicio Propuesta

*Fecha Fin Propuesta

*Etapa Competencia

*Fecha de Entrega

*Fecha de Apertura

OBS: SE ACLARA QUE LAS FECHAS SE ENCUENTRAN PUBLICADAS EN EL SICP.

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

DATOS DE LA LICITACIÓN

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

Contratación Pública Sostenibles - CPS

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

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

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

Criterios sociales y económicos:

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

Criterios ambientales:

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

Conducta empresarial responsable:

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

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

Difusión de los documentos de la licitación

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

Aclaración de los documentos de la licitación

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

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

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

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

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

Documentos de la oferta

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

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

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

Oferentes en consorcio

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

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

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

Aclaración de las ofertas

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

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

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

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

Disconformidad, errores y omisiones

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

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

Con la condición de que la oferta cumpla sustancialmente con los Documentos de la Licitación, la Convocante corregirá errores aritméticos de la siguiente manera y notificará al 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 total y el precio unitario será corregido.

2. Los precios subtotales podrán ser corregidos siempre que se mantenga inalterable el precio total obtenido en la SBE.

3. En ambos casos, los precios unitarios modificados no podrán ser superiores a los precios unitarios iniciales que figuran en el Acta de Sesión Pública Virtual de la SBE.

4. 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, aun cuando el resultado varíe del precio total que se encuentra en el Acta de Sesión Pública Virtual de la SBE como precio final.

5. 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:

SI, EN IDIOMA INGLES.

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:

- **Fecha:** Lunes y Viernes, desde el día de la publicación del llamado hasta un día antes de la fecha tope de consultas.
- **Hora de inicio:** 08:00hs
- **Hora de finalización:** 09:00hs
- **Lugar:** Edificio de la Dirección General de los Registros Públicos - Avda. Eusebio Ayala c/ Capitán Román García.
- **Procedimiento:** Los oferentes que quieran realizar la visita, deberán presentarse en el Departamento de Informática de la Dirección General de Registros Públicos, con una nota firmada por el representante legal de la empresa en la cual mencionan NOMBRE Y NUMERO DE CEDULA de la persona que realizará la visita, al término de cada visita se emitirá una constancia.
- **Nombre del funcionario responsable de guiar la visita:** Las visitas serán guiadas por técnicos del Dpto. de Informática de la Dirección General de Registros Públicos.
- **Participación obligatoria:** No, en caso de que el oferente conozca el sitio debe presentar una Declaración Jurada en la cual manifiesta que conoce las instalaciones.

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

El sistema de abastecimiento simultáneo para esta licitación será:

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:

PARA TODOS LOS ITEMS

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

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.

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 calendarios) por:

120

Las ofertas se deberán mantener válidas por el periodo indicado en el presente apartado, que se computará a partir del inicio de la etapa competitiva. Toda oferta con un periodo menor será rechazada.

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

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

Garantías: instrumentación, plazos y ejecución.

1. La garantía de mantenimiento de oferta deberá expedirse en un monto en guaraníes que no deberá ser inferior al porcentaje especificado en el SICP. El oferente puede adoptar cualquiera de las formas de instrumentación de las garantías dispuestas por las normativas vigentes.

2. La garantía de mantenimiento de ofertas presentada en los términos del párrafo anterior, deberá cubrir el precio total de la oferta en la etapa de recepción de propuestas.

3. 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.

4. En caso de instrumentarse a través de Garantía Bancaria, deberá estar sustancialmente de acuerdo con el formulario de Garantía de Mantenimiento de oferta incluido en la Sección "Formularios".

5. 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.

6. 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 oferente no presentare su oferta en la fecha y hora señaladas, previo requerimiento por parte de la convocante,

e) Si el adjudicatario no procede, por causa imputable al mismo a:

e.1. suministrar los documentos indicados en el pliego de bases y condiciones para la firma del contrato,

e.2. firmar el contrato,

e.3. suministrar en tiempo y forma la garantía de cumplimiento de contrato,

e.4. se comprobare que las declaraciones juradas presentadas por el oferente adjudicado con su oferta sean falsas,

e.5. el adjudicatario no presentare las legalizaciones correspondientes para la firma del contrato, cuando éstas sean requeridas, o

e.6. no se formaliza el consorcio por escritura pública, antes de la firma del contrato.

7. 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.

8. 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 cumplimiento deberá ser entregada antes del cumplimiento de la prestación.

9. 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:

150

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. Cuando la competencia se desarrolle por más de un día, la garantía de mantenimiento de oferta deberá cubrir a partir del primer día del inicio de la etapa competitiva.

Porcentaje de Garantía de Fiel Cumplimiento de Contrato

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

5,00 %

La garantía de Cumplimiento de Contrato deberá ser presentada por el provedor, 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:

42 (cuarenta y dos) meses contados desde el día de la firma del contrato.

Periodo de validez de la Garantía de los bienes

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

El oferente adjudicado al término de la puesta en funcionamiento de los equipos deberá presentar por escrito un certificado de garantía que tendrá una vigencia de 36 (treinta y seis) meses y cubrirá defectos de fabricación, fallos, soporte de atención de hardware, asistencia técnica y mano de obra.

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:

3 (tres) días hábiles desde el momento de la identificación y comunicación del problema vía correo electrónico o por nota a la empresa adjudicada. Si la solución demandara más de 3 (tres) días hábiles, el proveedor deberá notificar dentro de ese periodo vía correo electrónico o por nota el motivo de la demora y proporcionar un equipo de reemplazo idéntico o de características superiores al equipo con fallas y con EOL (end of life) superior a 5 (cinco) años, durante el tiempo que demore la reparación; sin ningún costo para la institución. El tiempo de reparación no podrá exceder 30 (treinta) días hábiles. En caso de que supere dicho plazo, el oferente adjudicado deberá reemplazarlo con otro equipo de iguales especificaciones técnicas o superiores al equipo adjudicado.

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 guaranies, 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

Las ofertas serán presentadas en un solo sobre y 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;

4. Llevar una advertencia de no abrir antes de la hora y fecha de apertura de ofertas.

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

Culminada la etapa competitiva, presentarán las ofertas físicas en la dirección y hasta la fecha y hora que se indican en el SICP, los siguientes participantes requeridos:

TODOS LOS OFERENTES

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 oferta sea electrónica la misma 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.

3. Primero se procederá a verificar de entre las ofertas recibidas por courrier 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. 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.

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".

Adicionalmente a lo establecido en el párrafo anterior el oferente deberá considerar las siguientes condiciones de participación:

Que se encuentren registrados/as en el Sistema de Información de Proveedores del Estado (SIPE), debiendo suscribir ante el mismo una Declaración Jurada en la cual manifiesta que tiene pleno conocimiento y acepta las reglas del proceso para su activación como oferente. La Declaración Jurada referida, podrá ser descargada desde el SICP, módulo del SIPE.

Que activados/as conforme al SIPE posean su Usuario y Contraseña, personal e intransferible, salvo que los mismos hayan sido cancelados por el Sistema, de conformidad a la reglamentación específica. La pérdida del usuario y contraseña deberá ser comunicada a la DNCP para que, a través del Sistema, sea bloqueado el acceso inmediatamente; y

Como requisito para la participación en la Subasta a la Baja Electrónica, el oferente deberá manifestar en el campo previsto en el Sistema Electrónico, que cumple plenamente los requisitos de habilitación y que su propuesta de precios está conforme con las exigencias del pliego de bases y condiciones.

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 Nº 2051/03, modificado por Ley Nº 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 Nº 2051/03, modificado por Ley Nº 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 Nº 2051/03, modificado por Ley Nº 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 Nº 2051/03, modificado por Ley Nº 6716/2021, aparecen en la base de datos del SINARH o de la Secretaría de la Función Pública.
4. Si se constatara 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 Nº 2051/03, modificado por Ley Nº 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, 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 de la etapa competitiva.

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.

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 (*) **SUSTANCIAL** [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 (*) **SUSTANCIAL** La garantía de mantenimiento de oferta debe ser extendida, bajo la forma de una garantía bancaria o póliza de seguro de caución.
3. Certificado de Cumplimiento con la Seguridad Social. (**)
4. Certificado de Producto y Empleo Nacional, emitido por el MIC, en caso de contar. (**)
5. Constancia de presentación de la Declaración Jurada de bienes y rentas, activos y pasivos ante la Contraloría General de la República, para los sujetos obligados según los incisos a) y b) del numeral 2 del art. 1 de la Ley N° 6355/19. (**) **NO APLICA**
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.
• Fotocopia simple de la Cédula de Identidad del firmante de la oferta. (*) **SUSTANCIAL**
• Constancia de inscripción en el Registro Único de Contribuyentes - RUC. (*) **SUSTANCIAL**
• 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. (*) **SUSTANCIAL**
9.2. Oferentes Individuales. Personas Jurídicas.
• 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. (*) **SUSTANCIAL**
• 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.
• 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. (*) **SUSTANCIAL**
9.3. Oferentes en Consorcio.
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. (*) **SUSTANCIAL**
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). (*) **SUSTANCIAL**

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

- 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 (*): **SUSTANCIAL**

1. 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
2. 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 al inicio de la etapa competitiva.

Capacidad Financiera

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

a. Para contribuyente de IRE.

Deberán cumplir con los siguientes parámetros:

Ratio de Liquidez: activo corriente / pasivo corriente

Deberá ser igual o mayor que 1, en promedio, en los años 2020, 2021, 2022.

Endeudamiento: pasivo total/ activo total

No deberá ser mayor a 0,80 en promedio, en los años 2020, 2021, 2022.

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

El promedio de la sumatoria de los años 2020, 2021, 2022, no deberá ser negativo.

b. Para contribuyentes de IRE SIMPLE.

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso) Deberá ser igual o mayor que 1, el promedio de la sumatoria de los años 2020, 2021, 2022.

c. Para contribuyentes de IRP

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio de la sumatoria de los años 2020, 2021, 2022.

d. Para contribuyentes de exclusivamente IVA General

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso). Deberá ser igual o mayor que 1, el promedio de la sumatoria de los años 2020, 2021, 2022.

- **OFERENTES EN CONSORCIO: Cada miembro debe cumplir con cada uno de los requisitos.**

Requisitos documentales para la evaluación de la capacidad financiera

a. Balance General y Estados de Resultados (comparativo) de los años 2020, 2021, 2022, firmados por el contador, propietario y/o representante legal si correspondiere, acorde a las normas contables y a los modelos establecidos en las Normativas Vigentes de la Direccion Nacional de Ingresos Tributarios, que se encuentran en la página web (www.set.gov.py).

b. Formulario 500 para los años 2020,2021 y 2022 correspondientes a la Declaración Jurada del Impuesto a la Renta.

c. Formulario 501 para los años 2020, 2021 y 2022 correspondientes a contribuyentes del IRE SIMPLE.

d. Formulario 515 para contribuyentes de Renta Personal y Formulario 516 IRP - RGC para los años 2020,2021 y 2022.

e. Formulario 120 solo para contribuyentes del IVA General de los últimos 36 (TREINTA Y SEIS) meses, correspondiente a los años 2020, 2021 y 2022.

Experiencia requerida

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

1. El oferente deberá contar con contratos ejecutados y/o facturas de ventas relacionados a la **VENTA, INSTALACIÓN Y/O CONFIGURACIÓN DE EQUIPOS DE REDES** que podrán corresponder tanto a empresas públicas como privadas, acompañados de los documentos que avalen el cumplimiento satisfactorio. Dichos contratos deberán corresponder al periodo comprendido entre los años 2020, 2021 y 2022 y deberá ser como mínimo el 50% (cincuenta por ciento) del monto total ofertado. Se aclara que no es necesario contar con un contrato por año.
2. El oferente deberá contar con al menos 3 (tres) años de antigüedad en el rubro del sector tecnológico.

- **OFERENTES EN CONSORCIO:** El socio líder debe cumplir al menos con el 60% (sesenta por ciento) del requisito y los demás socios en su conjunto al menos el 40% (cuarenta por ciento) de este requisito.

Requisitos documentales para la evaluación de la experiencia

1. Copias de contratos ejecutados y/o facturas de ventas relacionados a la **VENTA, INSTALACIÓN Y/O CONFIGURACIÓN DE EQUIPOS DE REDES** que podrán corresponder tanto a empresas públicas como privadas, acompañados de los documentos que avalen el cumplimiento satisfactorio. Dichos contratos deberán corresponder al periodo

comprendido entre los años 2020, 2021 y 2022 y deberá ser como mínimo el 50% (cincuenta por ciento) del monto total ofertado. Se aclara que no es necesario contar con un contrato por año.
2. Copia de constitución en caso de sociedades o la constancia del RUC en caso de empresas unipersonales.

Capacidad Técnica

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

1. Deberá contar con al menos 4 (cuatro) técnicos certificados en las marcas de los ítems ofertados, de los cuales, 2 (dos) técnicos con certificación de nivel superior y 2 (dos) técnicos con certificación de nivel medio. Los mismos deberán formar parte del plantel de la empresa.

2. El oferente deberá contar con la autorización del fabricante o representante de la marca de los bienes ofertados para su comercialización local.

3. Los equipos ofertados deberán contar con Certificación de Calidad ISO 9001:2015 o similar. El mismo deberá ser mínimamente para fabricación. No se aceptarán certificados de ensamblaje de equipos.

4. Manifestar que cuenta con Centros Autorizados de Servicio (CAS) en el país.

5. Manifestar que será de entera responsabilidad del oferente, todos los daños a los bienes de la convocante, provenientes de hechos u omisiones voluntarios o involuntarios, resultantes de la negligencia o impericia de sus empleados, sin cargo alguno para la convocante.

6. Visita e inspección técnica en el edificio de la Dirección General de los Registros Públicos. En caso de no realizar la visita deberá presentar declaración jurada en la cual manifiesta que conoce las instalaciones.

7. Cumplir con las especificaciones técnicas solicitadas.

8. Contar con catálogo de los bienes ofertados.

9. El oferente deberá garantizar que todos los bienes ofertados a la convocante son nuevos y sin uso.

- **OFERENTES EN CONSORCIO:** Los integrantes del consorcio en forma combinada deben cumplir con todos los requisitos solicitados.

Requisito documental para evaluar la capacidad técnica

1. Listado de técnicos acompañado de la Planilla del Instituto de Previsión Social correspondiente al mes anterior vencido a la fecha de la etapa competitiva en donde figuren los técnicos propuestos, los cuales deberán formar parte del plantel de la empresa.

a. 2 (dos) técnicos con certificación de nivel superior de las marcas de los equipos de comunicación ofertadas (Ej.: Cisco CCNP, Fortinet NSE7, Sonicwall SNSP, Huawei HCIP).

b. 2 (dos) técnicos con certificación de nivel medio de las marcas de los equipos de comunicación ofertadas (Ej.: Cisco CCNA, Fortinet NSE4, Sonicwall SNSA, Huawei HCIA).

El referido listado deberá estar acompañado de la siguiente documentación:

- Currículum Vitae de los técnicos propuestos acompañado de todos los documentos respaldatorios que avalen la formación profesional.

- Copia de certificado de capacitación en la marca ofertada.
- Copia de cédula de identidad de los técnicos.

2. Autorización del fabricante en idioma español o inglés debidamente traducido por traductor publico matriculado, para representantes, distribuidores y sub - distribuidores de los productos ofrecidos.

Para Representantes debe reunir los siguientes requisitos:

Documentación expedida por el Fabricante que los acredite como representante de la marca, dichos documentos deben estar debidamente legalizados por el Consulado Paraguayo del País de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay. Los mismos deben ser originales o copias autenticadas por Escribano Público.

Para Distribuidor Autorizado debe reunir los siguientes requisitos:

Documentación expedida por el Fabricante que los acredite como distribuidor autorizado de la marca ofertada para tal efecto debe presentar el documento original o copia autenticada por Escribano Público, y el mismo debe estar debidamente legalizado por el Consulado Paraguayo del País de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay.

Para Sub-Distribuidor debe reunir los siguientes requisitos:

Documento original o copia autenticada por Escribano Público de la autorización del Fabricante extendida al Representante, Distribuidor y/o Resellers para el PARAGUAY Y/O LATINOAMERICA que lo nombra como representante, o distribuidor autorizado de la marca ofertada en la cual lo autoriza a nombrar sub - distribuidores. Para tal efecto debe presentar el documento original o copia autenticada por Escribano Público, y el mismo debe estar debidamente legalizado por el Consulado Paraguayo del País de emisión del documento y del Ministerio de Relaciones Exteriores de la República del Paraguay.

Serán considerados válidos los documentos apostillados como los documentos legalizados por el Consulado y el Ministerio de Relaciones Exteriores en conformidad a la **Ley N° 4987/13 QUE APRUEBA EL CONVENIO SUPRIMIENDO LA EXIGENCIA DE LA LEGALIZACIÓN DE LOS DOCUMENTOS PÚBLICOS EXTRANJEROS.**

3. Certificación de Calidad ISO 9001:2015 o similar. El mismo deberá ser mínimamente para fabricación de los equipos ofertados. No se aceptarán certificados de ensamblaje de equipos.

4. Declaración jurada por la cual el oferente manifieste cuales son los Centros Autorizados de Servicio (CAS) en el país.

5. Declaración jurada en la cual el oferente manifiesta que será de su entera responsabilidad, todos los daños a los bienes de la convocante, provenientes de hechos u omisiones voluntarios o involuntarios, resultantes de la negligencia o impericia de sus empleados, sin cargo alguno para la convocante.

6. Constancia de visita e inspección a las instalaciones de la Dirección General de los Registros Públicos. En caso de no realizar la visita deberá presentar declaración jurada en la cual manifiesta que conoce las instalaciones.

7. Especificaciones técnicas ofertadas.

8. Catálogos en los cuales se detallan claramente todas las especificaciones técnicas de los bienes ofertados. Los catálogos deben coincidir con las especificaciones técnicas ofrecidas, y deberán ser presentados en idioma español o inglés. En caso de encontrarse en otros idiomas, deberán estar debidamente traducidos por traductor público matriculado. Debe adjuntarse una copia en formato PDF.

9. Declaración jurada en la cual el oferente garantiza que todos los bienes ofertados a la convocante son nuevos y sin uso.

Criterio de desempate de ofertas

El vencedor de cada grupo subastado será el oferente que ingresó el menor precio. En los casos de igualdad de precios, queda como vencedor el que lo haya ingresado primero.

Siempre que el criterio de desempate establecido, no sea aplicable, 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.

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 serán suministrados por el Proveedor como si hubiesen sido expresamente mencionados, salvo disposición contraria en el Contrato.

Los bienes 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.

Detalle de los productos con las respectivas especificaciones técnicas

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

Detalle de los productos con las respectivas especificaciones técnicas

LOTE N° 1 - ADQUISICIÓN DE SWITCHES				
ITEM	**DESCRIPCIÓN**	**CANTIDAD**	**UNIDAD DE MEDIDA**	**PRESENTACIÓN**
1	SWITCHES DE CORE	2	UNIDAD	UNIDAD
2	SWITCHES DE DATA CENTER	3	UNIDAD	UNIDAD
3	SWITCHES DE ACCESO	20	UNIDAD	UNIDAD

LOTE N° 2 ADQUISICIÓN DE EQUIPOS DE SEGURIDAD FORTINET				
1	SOLUCIÓN ANTISPAM Y SEGURIDAD PARA CORREO **FORTINET FORTIMAIL**	2	UNIDAD	UNIDAD
2	CORTAFUEGOS DE APLICACIONES WEB **FORTINET FORTIWEB**	2	UNIDAD	UNIDAD

Alcance de los trabajos y servicios

Los oferentes deberán entregar todos los bienes y servicios del presente llamado en la modalidad de llave en mano, por lo que deberán considerar todos los equipamientos, accesorios, materiales de instalación, horas de servicio técnico especializado, etc., para la correcta implementación de la solución ofertada, de acuerdo con los requerimientos técnicos indicados en el presente documento.

Entre los servicios que se identifican y se mencionan de manera enunciativa pero no taxativa se encuentran:

- Desinstalar y desmontar los equipos actualmente utilizados y ubicados en sus respectivos gabinetes.
- Instalar y conectorizar todos los nuevos equipos adquiridos.
- Actualizar el sistema operativo de los equipos proveídos a la última versión disponible.
- Arreglar, reemplazar, etiquetar y/o identificar los cables, para el correcto montaje de los nuevos equipos.
- Configurar los nuevos equipos montados y los ya existentes, a fin de lograr la interconexión necesaria para el uso y acceso a la red y servicios.
- Todos los dispositivos conectados deberán contar con enlaces redundantes para prevenir interrupciones en el servicio.
- Documentación técnica que contenga el diagrama físico, diagrama lógico, etiquetado y certificación del esquema del despliegue de la red de datos.
- Realizar la transferencia tecnológica por cada ítem solicitado.
- Además, los switches del LOTE 1 ITEM 1,2 Y 3 deberán ser de la misma marca o fabricante de tal manera a garantizar interoperabilidad y gestión unificada centralizada.

El proveedor deberá prever horas/técnico bajo demanda, de acuerdo con las necesidades de la entidad convocante, con el fin de atender reclamos, realizar configuraciones adicionales o abordar cualquier otra necesidad identificada y requerida.

Corresponde mencionar que los servicios de instalación, montaje, configuración y todo lo necesario para la puesta en funcionamiento de los equipos e infraestructura de red de datos deberán ser realizados por los técnicos propuestos, cuya documentación fuera proveída en el momento de la oferta, salvo casos excepcionales y debidamente justificados. Para estos casos, el técnico propuesto por la empresa deberá tener el mismo o mejor perfil que el reemplazado y estará sujeto a aprobación por parte de la Convocante.

Asimismo, el proveedor se compromete a reemplazar partes cambiables de los equipos que presenten fallas identificadas, como, por ejemplo, fuentes de poder, módulos de expansión, GBIC's, SFP, etc.

Por lo que se requiere lo detallado a continuación:

LOTE N° 1 - ADQUISICIÓN DE SWITCHES

ITEM N° 1: Switch de CORE

Se deberá contemplar la provisión de 2 (dos) switches de core administrables de 24 puertos a 10Gbase X con 2 puertos uplink a 100 GB cada uno, módulos o adaptadores para disponibilizar el stack o apilamiento (vss, virtual chassis o semejante) y módulos SFP+ 10 GB para los enlaces verticales de FO (switches de acceso, proveedores y data center) y dispositivos de seguridad (cortafuegos WAF y seguridad de correo) **(Lote N° 2, ÍTEM 1 y 2).**

Los equipos suministrados deberán configurarse en un esquema de alta disponibilidad (HA), garantizando la continuidad de la operatividad de la red en caso de que uno de los switches presente una falla.

ITEM N°2: Switch de DATA CENTER

Se deberá contemplar la provisión de 3 (tres) switches administrables de 48 puertos cada uno, cuatro interfaces de uplink, módulos o adaptadores para disponibilizar el stack o apilamiento (vss, virtual chassis o semejante) y módulos SFP+ 10GB

para los enlaces de FO con los Switches de CORE **(ITEM 1)**.

ITEM N° 3: Switches de ACCESO

Se deberá contemplar la provisión de 20 (veinte) switches administrables de acceso de 48 puertos cada uno, cinco de ellos con soporte POE, cuatro interfaces de uplink a 10 GB, módulos o adaptadores para disponibilizar el stack o apilamiento (vss, virtual chassis o semejante) y módulos SFP+ 10 GB para los enlaces verticales a través de FO a los Switches CORE **(ITEM 1)**.

Ubicación	Cantidad		Subtotal
	Sin POE	Con POE	
PLANTA BAJA	4	1	5
ENTREPISO	3	1	4
PRIMER PISO	6	1	7
SEGUNDO PISO	1	1	2
TERCER PISO	0	1	1
CUARTO PISO	0	1	1
TOTAL	**14**	**6**	**20**

Observaciones:

Actualmente ya se encuentran desplegados los enlaces verticales a los distintos pisos a través de fibra óptica multimodo, todos conectorizados a sus respectivos DIO.

LOTE N° 2 ADQUISICIÓN DE EQUIPOS DE SEGURIDAD FORTINET

ITEM N° 1 : Solución antispam y seguridad para correo electrónico

Se requieren 02 (dos) dispositivos capaces de ofrecer una robusta solución para garantizar la integridad y confidencialidad de las comunicaciones electrónicas en la Institución. A continuación, se presentan detalles, descripciones y características claves que deben cumplir los equipos.

Seguridad Integral: Defensa integral contra las amenazas de correo electrónico, incluyendo malware, phishing y ataques dirigidos.

Filtrado Avanzado: Técnicas de filtrado para detectar y bloquear correos no deseados y peligrosos.

Análisis Heurístico: Para identificar amenazas desconocidas basadas en comportamientos sospechosos.

Detección de Contenido: Escanea los mensajes en busca de contenido sensible o violaciones de políticas predefinidas.

Prevención de Fuga de Datos: Protege a la organización contra la fuga de información confidencial a través del correo electrónico.

Rendimiento Eficiente: Alto rendimiento para gestionar grandes volúmenes de correos electrónicos de manera eficiente.

Alta Disponibilidad: Garantizar la disponibilidad continua del servicio de correo electrónico para evitar interrupciones en la comunicación (HA).

Actualizaciones en Tiempo Real: Mantener una base de datos actualizada de amenazas para una protección en tiempo real.

Gestión Centralizada: Administración centralizada de políticas de seguridad de correo electrónico.

Informes Detallados: Informes detallados sobre el tráfico de correo y las amenazas bloqueadas.

Estas características son requeridas con el objeto de salvaguardar la integridad y seguridad de la comunicación por correo electrónico, brindando una protección confiable y actualizada contra las crecientes amenazas cibernéticas.

Ambos dispositivos se deben de configurar en un esquema de Alta Disponibilidad (HA) en caso de que uno de los mismos presente una falla.

Para garantizar la compatibilidad de las funciones requeridas, el equipo deberá ser del mismo fabricante del actual **FIREWALL/UTM** y **ANALIZADOR DE LOGS** con que cuenta la Institución, **FORTINET FORTIGATE 200F y FORTIANALYZER VM** , o en su defecto contar con un respaldo documental de interoperabilidad de las funciones de administración centralizada, de gestión de reportes, entre otros. Es decir, ambos fabricantes deberán garantizar mediante nota dirigida a la Convocante la interoperabilidad entre equipos.

ITEM N° 2: Cortafuegos de aplicaciones web

Se requieren 02 (dos) dispositivos capaces de brindar una solución de seguridad de red diseñada para proteger aplicaciones web críticas contra amenazas cibernéticas. Su enfoque está en garantizar la integridad, confidencialidad y disponibilidad de los datos que circulan a través de aplicaciones web. A continuación, se presentan detalles, descripciones y características claves que deben cumplir los equipos.

Protección en Tiempo Real: Defensa en tiempo real contra amenazas web, incluyendo ataques de inyección SQL, cross-site scripting (XSS), y otros ataques comunes.

Detección y Prevención de Ataques: Técnicas avanzadas de detección de intrusos para identificar y prevenir amenazas antes de que afecten las aplicaciones.

WAF (Web Application Firewall): Inspeccionar y filtrar tráfico HTTP/HTTPS para proteger aplicaciones contra ataques y vulnerabilidades conocidas.

Balanceo de Carga y Disponibilidad: Garantizar el acceso continuo a las aplicaciones, incluso en situaciones de alto tráfico.

Optimización de Rendimiento: Optimizar el rendimiento de aplicaciones web al reducir la latencia y acelerar la entrega de contenido.

Gestión Centralizada: Permitir una gestión centralizada y sencilla de las políticas de seguridad a través de una interfaz intuitiva.

Escalabilidad: Escalable para adaptarse a las necesidades de crecimiento de las aplicaciones y la red.

Integración de Informes y Análisis: Proporcionar informes detallados y herramientas de análisis para evaluar la eficacia de las políticas de seguridad.

Actualizaciones Continuas: Actualizaciones periódicas que mantienen la protección actualizada contra las amenazas emergentes.

Alta Disponibilidad: Ofrece opciones para configuraciones de alta disponibilidad, asegurando la continuidad de las operaciones.

Estas características son requeridas para contar con una solución sólida, garantizar la seguridad y el rendimiento de las aplicaciones web proveídas por la Institución.

Ambos dispositivos se deben de configurar en un esquema de Alta Disponibilidad (HA) en caso de que uno de los mismos presente una falla.

Para garantizar la compatibilidad de las funciones requeridas, el equipo deberá ser del mismo fabricante del actual **FIREWALL/UTM** y **ANALIZADOR DE LOGS** con que cuenta la Institución, **FORTINET FORTIGATE 200F y FORTIANALYZER VM** , o en su defecto contar con un respaldo documental de interoperabilidad de las funciones de administración centralizada, de gestión de reportes, entre otros. Es decir, ambos fabricantes deberán garantizar mediante nota dirigida a la Convocante la interoperabilidad entre equipos.

A continuación, se listan de manera enunciativa y no limitativa las Especificaciones Técnicas consideradas dentro del alcance del presente proyecto, donde todos los ítems y accesorios deberán ser compatibles entre sí, garantizando su correcta interoperabilidad:

LOTE N° 1 ADQUISICIÓN DE SWITCHES

ITEM 1 - SWITCHES DE CORE

Nro.	Descripción	Requerimiento mínimo exigido
1	Marca	indicar
2	Modelo	indicar
3	Procedencia	indicar
4	Cantidad	2 (dos)
5	Descripcion	Switch de Core
6	Stacking/Apilamiento: minima cantidad de equipos apilables	≥ 2
7	Tipo de uso	Core
	RENDIMIENTO Y CAPACIDAD	
8	Capacidad mínima de forwarding soportado por equipo	≥ 490Mpps
9	Capacidad mínima de conmutación soportada por equipo	≥ 1050 Gbps
10	Capacidad mínima de forwarding entre módulos o miembros del stacking (backplane) soportado por equipo	≥ 300 Gbps
11	El equipo deberá estar equipado con la cantidad de Memoria RAM y FLASH mínima necesaria para soportar todas las funcionalidades de la última versión del sistema operativo en el momento de la entrega del equipo y los requerimientos de prestaciones y performance solicitadas en estas especificaciones técnicas.	RAM/ DRAM ≥ 4GB
12	MTBF Mínimo Requerido	≥ 320.000 Hs.
	INTERFACES	
13	Cantidad mínima de interfaces 40/100GbE QSFP28 independientes instalados	≥ 2
14	Cantidad mínima de interfaces de 10 GbE ópticas instaladas (independientes de los items anteriores)	≥ 24
15	Capacidad de crecimiento mínima en interfaces de 10GbE y/o 25GbE	≥ 4 (opcional)
16	Cantidad mínima de puertos Serial independiente para administración fuera de banda del equipo.	≥ 1 (opcional)
17	Cantidad mínima de puertos RJ-45 para ser usado como consola de administración.	≥ 1

18	modulos SFP+ FO (a incluir) para velocidades 10Gbps	32 en total (16 por equipo)
19	patchcord FO (a incluir)	32 en total (16 por equipo)
	Stacking/Apilamiento	
20	Vinculación de equipos por puertos con interfaces que soporten mínimo 40GbE	EXIGIDO
21	Configuración desde una única dirección IP y para su administración actuarán como un único equipo.	EXIGIDO
22	El reemplazo de un miembro del stack deberá ser no disruptivo. En caso que la versión de Sistema Operativo del equipo a incorporar sea distinta de la vigente el stack/Virtual Chasis , la misma deberá poder actualizarse automáticamente desde el equipo controlador del stack/Master del Virtual Chasis	EXIGIDO
23	Capacidad de conformar un único equipo desde el punto de vista de la administración	EXIGIDO
24	Mínimo de equipos agrupados para administrar con un único acceso administrativo	≥ 4
25	Los puertos miembros de un grupo de Link Aggregation (802.3ad) LAG deben poder pertenecer a diferentes miembros del Stack	EXIGIDO
	FUNCIONES SWITCH DE RED	
26	Todas las interfaces se podrán utilizar independientemente en modo L3 o L2 , es decir se podrán agrupar para formar un dominio de Broadcast (L2) representadas por una interfase L3 virtual (Interfase VLAN) o cada interfase física o lógica podrá configurarse con una dirección IP independiente (L3)	EXIGIDO
27	Funcionalidad de Servidor DHCP	EXIGIDO
28	Funcionalidad de Cliente DHCP	EXIGIDO
29	Funcionalidad de DHCP Relay y Helper	EXIGIDO
30	Protocolo de enrutamiento RIPv1, RIPv2	EXIGIDO
31	Capacidad de soporte para Protocolo de enrutamiento OSPF v2, v3	EXIGIDO
32	Soporte de Bidirectional Forwarding Detection (BFD) con instalacion futura de licencia correspondiente	EXIGIDO
33	Soporte de protocolo de enrutamiento BGP	EXIGIDO

34	Soporte de protocolo de encapsulamiento VXLAN	EXIGIDO
35	Debe soportar la funcionalidad de ruteo por distintos campos del paquete IP como Origen/Destino o puertos (Policy Based Routing o Filter Based Routing) en forma independiente a la tabla de ruteo por defecto	EXIGIDO
36	Mínimo VLANS soportadas 802.1q Vlan Tagging	≥ 4092
37	Mínimo de direcciones MAC	≥ 112000
38	Mínimo de rutas IPv4 unicast	≥ 130000
39	Mínimo de rutas multicast IPv4	40000
40	Multiple VLAN Registration Protocol (802.1ak)	EXIGIDO
	MULTICAST	
41	Los switches deberán tener la capacidad de interactuar con tráfico multicast para ello deberán soportar los siguientes protocolos :	EXIGIDO
42	IGMP Snooping	EXIGIDO
43	Capacidad de Soporte de IGMP v1 v2 y v3	EXIGIDO
44	Soporte PIM (Protocol Independant Multicast) en modo Sparse, SSM y DM	EXIGIDO
45	Capacidad de Soporte de protocolo MSDP (Multicast Source Discovery Protocol)	EXIGIDO
	ENRUTAMIENTO	
46	RIP v1 y v2	EXIGIDO
47	OSPF v2 y v3	EXIGIDO
48	BGP	EXIGIDO
49	VXLAN	EXIGIDO
	Management	
50	Syslog, Telnet, SSH	EXIGIDO
51	Neighbor DiscoveryProtocol	EXIGIDO
52	IPv6 ping	EXIGIDO
53	MLDv1 v2	EXIGIDO
	CALIDAD DE SERVICIO	

54	Mínimo de colas por hardware de calidad de servicio por interfase	12
55	Configuración por políticas de Calidad de Servicio asociando y marcando el tráfico a una determinada Clase de Servicio:	EXIGIDO
56	por Interfase	EXIGIDO
57	por dirección MAC	EXIGIDO
58	por campo 802.1p	EXIGIDO
59	por VLAN	EXIGIDO
60	por dirección IP origen y/o Destino	EXIGIDO
61	por campo DSCP/IP precedente	EXIGIDO
62	por puertos TCP/UDP	EXIGIDO
63	Configurar la Priorización del tráfico Saliente para cada clase de Servicio	EXIGIDO
	SEGURIDAD	
64	Limitar la cantidad de Direcciones MAC por puerto.	EXIGIDO
65	Deberá soportar MACSEC	EXIGIDO
66	Dynamic ARP inspection (DAI)	EXIGIDO
67	Deberá soportar Local Proxy ARP	EXIGIDO
68	Debera soportar Proxy ARP por VLAN	EXIGIDO
69	Deberá soportar DHCP Snooping	EXIGIDO
70	Deberá soportar Static ARP	EXIGIDO
	CONTROL DE ACCESO Y AUTENTICACION	
71	Cantidad mínima de ACL basadas en el puerto aplicadas al ingreso de los paquetes.	2048
72	Cantidad mínima de ACL basadas en el VLAN aplicadas al ingreso de los paquetes.	2048
73	Funcionalidad de 802.1x en cada por puerto.	EXIGIDO
74	Múltiples suplicantes en un mismo puerto físico validándolos en forma independiente.	EXIGIDO
75	Integración con sistemas de control de acceso por medio del protocolo RADIUS y 802.1x para autenticación de usuario.	EXIGIDO

76	El estándar 802.1X está basado en EAP (Extensible Authentication Protocol). Los switches deberán soportar los siguientes métodos de EAP:	EXIGIDO
77	EAP-MD5	EXIGIDO
78	EAP-TLS	EXIGIDO
79	EAP-TTLS	OPCIONAL
80	EAP-PEAP	EXIGIDO
81	Una vez que los dispositivos son autenticados podrán recibir parámetros, vía atributo de RADIUS, de las Listas de Acceso correspondientes.	EXIGIDO
82	Autenticación por dirección MAC sobre un servidor Radius.	EXIGIDO
83	Asignar VLAN cuando la autenticación fue realizada por Dirección MAC	EXIGIDO
84	Autenticación mediante portal cautivo	EXIGIDO
	FUNCIONES DE ALTA DISPONIBILIDAD	
85	Deberá soportar la agregación de interfaces para formar un único link, esta técnica es conocida como LAG (Link Aggregation Group) bajo la norma 802.3ad	EXIGIDO
86	Cantidad mínima de grupos LAG por sistema	≥ 126
87	Cantidad mínima de puertos pertenecientes a grupos LAG	≥ 16
88	Soporte de LACP - Link Aggregation Control Protocol	EXIGIDO
89	Mecanismo de protección contra loops de L2: 802.1D (Spanning Tree), 802.1w (Rapid Spanning Tree) y 802.1s (Multiple Spanning Tree)	EXIGIDO
	ADMINISTRACION	
90	Configuración por línea de comandos vía Telnet, SSHv2 y Serial	EXIGIDO
91	Configuración vía https	EXIGIDO
92	Monitoreo remoto mediante SNMP v1, v2 y v3	v2c, v3
93	Autenticación de usuarios de administración	Local, RADIUS y TACACS+
94	No debe almacenar el password de los administradores localmente , se debe generar un hash MD5 o SHA1 en configuración local	EXIGIDO

95	Cantidad mínima de configuraciones anteriores a almacenar automáticamente con fines de auditoría	25
96	Soporte configuración de rescate almacenada especialmente por el administrador	EXIGIDO
97	Permitirá deshacer cambios de configuración que no se confirmen dentro de un plazo prestablecido	EXIGIDO
98	Permitirá la configuración de funciones de RMON (RFC 2819)	EXIGIDO
99	Soporte de sFlow con sampling/muestreo sobre tráfico entrante y saliente	EXIGIDO
100	Capacidad de Soportar la función de envío de pruebas para evaluar el desempeño en tiempo real de la red (RPM)	EXIGIDO
	NORMAS Y ESTANDARES	
101	RFC 1122 Host Requirements	EXIGIDO
102	RFC 768 UDP	EXIGIDO
103	RFC 791 IP	EXIGIDO
104	RFC 783 TFTP	EXIGIDO
105	RFC 792 ICMP	EXIGIDO
106	RFC 793 TCP	EXIGIDO
107	RFC 826 ARP	EXIGIDO
108	RFC 894 IP over Ethernet	EXIGIDO
109	RFC 903 RARP	EXIGIDO
110	RFC 906 TFTP Bootstrap	EXIGIDO
111	RFC 1027 Proxy ARP	EXIGIDO
112	RFC 2068 HTTP server	EXIGIDO
113	RFC 1812 Requirements for IP Version 4 Routers	EXIGIDO
114	RFC 1519 CIDR	EXIGIDO
115	RFC 1256 IPv4 ICMP Router Discovery (IRDP)	EXIGIDO
116	RFC 1587 OSPF NSSA Option	EXIGIDO
117	RFC 1058 RIP v1	EXIGIDO
118	RFC 2453 RIP v2	EXIGIDO

119	RFC 1492 TACACS+	EXIGIDO
120	RFC 2138 RADIUS Authentication	EXIGIDO
121	RFC 2139 RADIUS Accounting	EXIGIDO
122	RFC 3579 RADIUS EAP support for 802.1x	EXIGIDO
123	RFC 2080 RIPng for IPv6	EXIGIDO
124	RFC 2154 OSPF w/Digital Signatures (password, MD-5)	EXIGIDO
125	RFC 5176 Dynamic Authorization Extensions to RADIUS	EXIGIDO
126	RFC 2030 SNTP, Simple Network Time Protocol	EXIGIDO
127	RFC 854 Telnet client and server	EXIGIDO
128	RFC 951, 1542 BootP	EXIGIDO
129	RFC 2338 VRRP	EXIGIDO
130	RFC 2131 BOOTP/DHCP relay agent and DHCP server	EXIGIDO
131	RFC 1591 DNS	EXIGIDO
132	RFC 2474 DiffServ Precedence	EXIGIDO
133	RFC 2598 DiffServ Expedited Forwarding (EF)	EXIGIDO
134	RFC 1981 Path MTU Discovery for IPv6	EXIGIDO
135	RFC 4915 MT-OSPF	EXIGIDO
136	RFC 2328 OSPF v2 (edge-mode)	EXIGIDO
137	RFC 2267 Network Ingress Filtering	EXIGIDO
138	RFC 2597 DiffServ Assured Forwarding (AF)	EXIGIDO
139	RFC 5643 OSPF v3 MIB support	EXIGIDO
	ALIMENTACION ELECTRICA, VENTILACION Y DIMENSIONES	
140	Tensión de operación Fuente de Alimentación 100-120V / 200-240V auto detectable.	EXIGIDO
141	Fuente de alimentación redundante soportado e incluido	EXIGIDO
142	Fuente de alimentación remplazable en caliente	EXIGIDO

143	Ventiladores redundantes	EXIGIDO
144	Ventiladores remplazables en caliente	EXIGIDO
145	Montaje en rack de 19	EXIGIDO
146	Cumplimiento de ROHS, EMC certification, Safety certification, Manufacturing certification	OPCIONAL
147	Temperatura de operación: 0°C a 45°C	EXIGIDO
148	Humedad de operación: 10% a 85% de humedad relativa máxima, sin condensación.	EXIGIDO
149	Cantidad de Unidad de Rack del Equipo	1U

ITEM 2 - SWITCHES DE DATA CENTER

Nro	Descripción	Requerimiento mínimo exigido
1	Marca	indicar
2	Modelo	indicar
3	Procedencia	indicar
4	Cantidad	3 (tres)
5	Descripcion	Switch de Datacenter
6	Tipo de uso	Data Center
	Rendimiento y capacidad	
7	Capacidad mínima de forwarding soportado por equipo	≥ 490Mpps
8	Capacidad mínima de conmutación soportada por equipo	≥ 800 Gbps
9	Capacidad mínima de forwarding entre módulos o miembros del stacking (backplane) soportado por equipo	≥ 300 Gbps
10	El equipo deberá estar equipado con la cantidad de Memoria RAM y FLASH mínima necesaria para soportar todas las funcionalidades de la última versión del sistema operativo en el momento de la entrega del equipo y los requerimientos de prestaciones y performance solicitadas en estas especificaciones técnicas.	RAM/ DRAM ≥ 4GB
11	MTBF Mínimo Requerido	≥ 87.600 Hs.
	Interfaces	

12	Cantidad mínima de interfaces ópticas Gigabit Ethernet independientes instalados	≥ 36
13	Cantidad mínima de interfaces 40/100GbE QSFP28 independientes instalados	≥ 2
14	Cantidad mínima de interfaces de 10 GbE ópticas instaladas (independientes de los items anteriores)	≥ 12
15	Capacidad de crecimiento mínima en interfaces de 10GbE y/o 25GbE	≥ 4
16	Cantidad mínima de puertos seriales independientes para administración fuera de banda del equipo.	≥ 1
17	Cantidad mínima de puertos RJ-45 para ser usado como consola de administración.	≥ 1
18	Modulos SFP+ FO (a incluir) para velocidades 10Gbps	24 en total (8 por equipo)
19	Modulos SFP a Cobre (a incluir) para velocidades 10Gbps	18 en total (6 por equipo)
20	Modulos SFP a Cobre (a incluir) para velocidades 1Gbps	72 en total (24 por equipo)
21	Patchcord FO (a incluir)	24 en total (8 por equipo)
	Stacking/Apilamiento	
22	Vinculación de equipos por puertos con interfaces que soporten mínimo 40GbE	EXIGIDO
23	Configuración desde una única dirección IP y para su administración actuarán como un único equipo.	EXIGIDO
24	El reemplazo de un miembro del stack deberá ser no disruptivo. En caso que la versión de Sistema Operativo del equipo a incorporar sea distinta de la vigente el stack/Virtual Chasis , la misma deberá poder actualizarse automáticamente desde el equipo controlador del stack/Master del Virtual Chasis	EXIGIDO
25	Capacidad de conformar un único equipo desde el punto de vista de la administración	EXIGIDO
26	Mínimo de equipos agrupados para administrar con un único acceso administrativo	≥ 2
27	Los puertos miembros de un grupo de Link Aggregation (802.3ad) LAG deben poder pertenecer a diferentes miembros del Stack	EXIGIDO
	FUNCIONES SWITCH DE RED	
28	Todas las interfaces se podrán utilizar independientemente en modo L3 o L2 , es decir se podrán agrupar para formar un dominio de Broadcast (L2) representadas por una interfase L3 virtual (Interfase VLAN) o cada interfase física o lógica podrá configurarse con una dirección IP independiente (L3)	EXIGIDO

29	Funcionalidad de Servidor DHCP	EXIGIDO
30	Funcionalidad de Cliente DHCP	EXIGIDO
31	Funcionalidad de DHCP Relay y Helper	EXIGIDO
32	Protocolo de enrutamiento RIPv1, RIPv2	EXIGIDO
33	Capacidad de soporte para Protocolo de enrutamiento OSPF v2, v3	EXIGIDO
34	Soporte de Bidirectional Forwarding Detection (BFD) con instalacion futura de licencia correspondiente	EXIGIDO
35	Soporte de protocolo de enrutamiento BGP	EXIGIDO
36	Soporte de protocolo de encapsulamiento VXLAN	EXIGIDO
37	Debe soportar la funcionalidad de ruteo por distintos campos del paquete IP como Origen/Destino o puertos (Policy Based Routing o Filter Based Routing) en forma independiente a la tabla de ruteo por defecto	EXIGIDO
38	Mínimo VLANS soportadas 802.1q Vlan Tagging	≥ 4000
39	Mínimo de direcciones MAC	≥ 100000
40	Mínimo de rutas IPv4 unicast	≥ 100000
41	Mínimo de rutas multicast IPv4	40000
42	Multiple VLAN Registration Protocol (802.1ak)	EXIGIDO
	MULTICAST	
43	Los switches deberán tener la capacidad de interactuar con tráfico multicast para ello deberán soportar los siguientes protocolos :	EXIGIDO
44	IGMP Snooping	EXIGIDO
45	Capacidad de Soporte de IGMP v1 v2 y v3	EXIGIDO
46	Soporte PIM (Protocol Independant Multicast) en modo Sparse, SSM y DM	EXIGIDO
47	Capacidad de Soporte de protocolo MSDP (Multicast Source Discovery Protocol)	EXIGIDO
	ENRUTAMIENTO	
48	RIP v1 y v2	EXIGIDO
49	OSPF v2 y v3	EXIGIDO
50	BGP	EXIGIDO

51	VXLAN	EXIGIDO
	Management	
52	Syslog, Telnet, SSH	EXIGIDO
53	Neighbor DiscoveryProtocol	EXIGIDO
54	IPv6 ping	EXIGIDO
55	MLDv1 v2	EXIGIDO
	CALIDAD DE SERVICIO	
56	Mínimo de colas por hardware de calidad de servicio por interfase	10
57	Configuración por políticas de Calidad de Servicio asociando y marcando el tráfico a una determinada Clase de Servicio:	EXIGIDO
58	por Interfase	EXIGIDO
59	por dirección MAC	EXIGIDO
60	por campo 802.1p	EXIGIDO
61	por VLAN	EXIGIDO
62	por dirección IP origen y/o Destino	EXIGIDO
63	por campo DSCP/IP precedente	EXIGIDO
64	por puertos TCP/UDP	EXIGIDO
65	Configurar la Priorización del tráfico Saliente para cada clase de Servicio	EXIGIDO
	SEGURIDAD	
66	Limitar la cantidad de Direcciones MAC por puerto.	EXIGIDO
67	Deberá soportar MACSEC	EXIGIDO
68	Dynamic ARP inspection (DAI)	EXIGIDO
69	Deberá soportar Local Proxy ARP	EXIGIDO
70	Debera soportar Proxy ARP por VLAN	EXIGIDO
71	Deberá soportar DHCP Snooping	EXIGIDO
72	Deberá soportar Static ARP	EXIGIDO
	CONTROL DE ACCESO Y AUTENTICACION	

73	Cantidad mínima de ACL basadas en el puerto aplicadas al ingreso de los paquetes.	2048
74	Cantidad mínima de ACL basadas en el VLAN aplicadas al ingreso de los paquetes.	2048
75	Funcionalidad de 802.1x en cada por puerto.	EXIGIDO
76	Múltiples suplicantes en un mismo puerto físico validándolos en forma independiente.	EXIGIDO
77	Integración con sistemas de control de acceso por medio del protocolo RADIUS y 802.1x para autenticación de usuario.	EXIGIDO
78	El estándar 802.1X está basado en EAP (Extensible Authentication Protocol). Los switches deberán soportar los siguientes métodos de EAP:	EXIGIDO
79	EAP-MD5	EXIGIDO
80	EAP-TLS	EXIGIDO
81	EAP-TTLS	OPCIONAL
82	EAP-PEAP	EXIGIDO
83	Una vez que los dispositivos son autenticados podrán recibir parámetros, vía atributo de RADIUS, de las Listas de Acceso correspondientes.	EXIGIDO
84	Autenticación por dirección MAC sobre un servidor Radius.	EXIGIDO
85	Asignar VLAN cuando la autenticación fue realizada por Dirección MAC	EXIGIDO
86	Autenticación mediante portal cautivo	EXIGIDO
	FUNCIONES DE ALTA DISPONIBILIDAD	
87	Deberá soportar la agregación de interfaces para formar un único link, esta técnica es conocida como LAG (Link Aggregation Group) bajo la norma 802.3ad	EXIGIDO
88	Cantidad mínima de grupos LAG por sistema	≥ 120
89	Cantidad mínima de puertos pertenecientes a grupos LAG	≥ 10
90	Soporte de LACP - Link Aggregation Control Protocol	EXIGIDO
91	Mecanismo de protección contra loops de L2: 802.1D (Spanning Tree), 802.1w (Rapid Spanning Tree) y 802.1s (Multiple Spanning Tree)	EXIGIDO
	ADMINISTRACION	

92	Configuración por línea de comandos vía Telnet, SSHv2 y Serial	EXIGIDO
93	Configuración vía https	EXIGIDO
94	Monitoreo remoto mediante SNMP v1, v2 y v3	v2c, v3
95	Autenticación de usuarios de administración	Local, RADIUS y TACACS+
96	No debe almacenar el password de los administradores localmente , se debe generar un hash MD5 o SHA1 en configuración local	EXIGIDO
97	Cantidad mínima de configuraciones anteriores a almacenar automáticamente con fines de auditoría	OPCIONAL
98	Soporte configuración de rescate almacenada especialmente por el administrador	EXIGIDO
99	Permitirá deshacer cambios de configuración que no se confirmen dentro de un plazo prestablecido	EXIGIDO
100	Permitirá la configuración de funciones de RMON (RFC 2819)	EXIGIDO
101	Soporte de sFlow con sampling/muestreo sobre tráfico entrante y saliente	EXIGIDO
102	Capacidad de Soportar la función de envío de pruebas para evaluar el desempeño en tiempo real de la red (RPM)	EXIGIDO
	NORMAS Y ESTANDARES	
103	RFC 1122 Host Requirements	EXIGIDO
104	RFC 768 UDP	EXIGIDO
105	RFC 791 IP	EXIGIDO
106	RFC 783 TFTP	EXIGIDO
107	RFC 792 ICMP	EXIGIDO
108	RFC 793 TCP	EXIGIDO
109	RFC 826 ARP	EXIGIDO
110	RFC 894 IP over Ethernet	EXIGIDO
111	RFC 903 RARP	EXIGIDO
112	RFC 906 TFTP Bootstrap	EXIGIDO
113	RFC 1027 Proxy ARP	EXIGIDO
114	RFC 2068 HTTP server	EXIGIDO
115	RFC 1812 Requirements for IP Version 4 Routers	EXIGIDO

116	RFC 1519 CIDR	EXIGIDO
117	RFC 1256 IPv4 ICMP Router Discovery (IRDP)	EXIGIDO
118	RFC 1587 OSPF NSSA Option	EXIGIDO
119	RFC 1058 RIP v1	EXIGIDO
120	RFC 2453 RIP v2	EXIGIDO
121	RFC 1492 TACACS+	EXIGIDO
122	RFC 2138 RADIUS Authentication	EXIGIDO
123	RFC 2139 RADIUS Accounting	EXIGIDO
124	RFC 3579 RADIUS EAP support for 802.1x	EXIGIDO
125	RFC 2080 RIPng for IPv6	EXIGIDO
126	RFC 2154 OSPF w/Digital Signatures (password, MD-5)	EXIGIDO
127	RFC 5176 Dynamic Authorization Extensions to RADIUS	EXIGIDO
128	RFC 2030 SNTP, Simple Network Time Protocol	EXIGIDO
129	RFC 854 Telnet client and server	EXIGIDO
130	RFC 951, 1542 BootP	EXIGIDO
131	RFC 2338 VRRP	EXIGIDO
132	RFC 2131 BOOTP/DHCP relay agent and DHCP server	EXIGIDO
133	RFC 1591 DNS	EXIGIDO
134	RFC 2474 DiffServ Precedence	EXIGIDO
135	RFC 2598 DiffServ Expedited Forwarding (EF)	EXIGIDO
136	RFC 1981 Path MTU Discovery for IPv6	EXIGIDO
137	RFC 4915 MT-OSPF	EXIGIDO
138	RFC 2328 OSPF v2 (edge-mode)	EXIGIDO
139	RFC 2267 Network Ingress Filtering	EXIGIDO
140	RFC 2597 DiffServ Assured Forwarding (AF)	EXIGIDO
141	RFC 5643 OSPF v3 MIB support	EXIGIDO
	ALIMENTACION ELECTRICA, VENTILACION Y DIMENSIONES	
142	Tensión de operación Fuente de Alimentación 100-120V / 200-240V auto detectable.	EXIGIDO

143	Fuente de alimentación redundante soportado e incluido	EXIGIDO
144	Fuente de alimentación remplazable en caliente	EXIGIDO
145	Ventiladores redundantes	EXIGIDO
146	Ventiladores remplazables en caliente	EXIGIDO
147	Montaje en rack de 19	EXIGIDO
148	Cumplimiento de ROHS, EMC certification, Safety certification, Manufacturing certification	OPCIONAL
149	Temperatura de operación: 0°C a 45°C	EXIGIDO
150	Humedad de operación: 10% a 85% de humedad relativa máxima, sin condensación.	EXIGIDO
151	Cantidad de Unidad de Rack del Equipo	1U

ITEM 3 - SWITCHES DE ACCESO

Nro.	Descripción	Requerimiento mínimo exigido
1	Marca	indicar
2	Modelo	indicar
3	Procedencia	indicar
4	Cantidad	20 (veinte)
5	Capacidad PoE y Power Budget	De los 20 (veinte) equipos solicidados, se requiere 5 (cinco) con capadidad PoE en sus 48 puertos con 750 watts de Power Budget
6	Descripcion	Switch de Acceso de 48 puertos
7	Tipo de configuracion de puertos	Fijos
8	Tipo de uso	Acceso a la Red
	Interfaces y rendimiento	
9	Interfaces independientes 10/100/1000BaseT-Cobre UTP RJ45	48 puertos RJ45
10	Interfaces SFP+ independientes (1/10Gbps)	4 puertos SFP+
11	Puerto 10/100 BaseT Ethernet adicional e independiente para administración del equipo (Out of Band Management)	1 puerto RJ45

12	Puerto SERIAL RS-232 para ser usado como consola de administración	Opcional
13	Puerto USB para el almacenado y descarga de configuraciones y sistema operativo	1 puerto USB
14	Throughput (Maximum with 64 Byte Packets)	130 Mpps
15	Capacidad de conmutacion por paquetes (unidirecional)	85 Gbps
16	Capacidad de conmutacion por paquetes (bidirecional)	170 Gbps
17	Modulos SFP+ FO (a incluir) para velocidades 10Gbps	60 en total (3 por equipo)
18	Patchcord FO (a incluir)	40 en total (2 por equipo)
	Stacking/Apilamiento	
19	Capacidad de backplane del Stack utilizando los puertos de UPLINK	40 Gbps
20	Equipos agrupados para administrar con un único acceso administrativo (mínimo)	≥ 2
21	Deberá soportar el protocolo Link Aggregation Control Protocol (LACP) IEEE 802.3ad.	Exigido
22	Numero de grupos a soportar por todo el STACK (mínimo)	128
	Calidad de Servicio	
23	Encolamiento basado en clases de servicio con priorización de trafico Strick priority en egreso	Exigido
24	Soporte de Port Shaping : puede ser usados para manjar el excesso de trafico, esta caracteristica define el ancho de banda maximo alojado en un puerto	Exigido
25	Soporte de queuing shaping: puede ser usados para manejar el exceso de trafico, esta caracteristica define el ancho de banda maximo alojado en cada cola	Exigido
26	Soporte de QoS en puertos LAG	Exigido
27	L2 QoS (classification, rewrite, queuing) Permite la clasificacion re-escritura y encolamiento de CoS en interfaces de layer 2.	Exigido
28	L3 QoS (classification, rewrite, queuing) Permite la clasificacion re-escritura y encolamiento de CoS en interfaces de layer 3	Exigido
29	Sopoorte de QoS Clasificacion , re-write y queueing en interfaces RVI (Interface VLANs)	Exigido
30	Soporta el tratamiento de las colas ante congestión con los mecanismos SDWRR (Shaped Deficit Weighted Round Robin) y SPQ (Strict Priority).	Exigido
31	Soporta el protocolo LLDP (Link Layer Discovery Protocol) IEEE 802.1AB y LLDP-MED (LLDP for Media Endpoint Device) ANSI/TIA-1057 integrado para Voice sobre IP (VoIP)	Exigido

32	Soporte de priorización de tráfico de salida por hardware mínimo ocho (8) colas de servicio por puerto.	Exigido
33	Politicas de trafico de red que limitan la velocidad de entrada y salida de una clase de trafico con base en el criterio establecido por el usuario. Permite control la velocidad maxima de trafico enviado o recibido en una interfaz y particionar una red en multiples nieles de clase de servicio	Exigido
34	Encolado estricto y de baja latencia (Strict priority queuing or Low Latency Queuing (LLQ)Strict priority queuing, or low latency queuing (LLQ): es una caracteristica usada para reeenviar de forma mas rapida ciertos tipos de trafico sensible a retardos (voz, video etc)	Exigido
35	Trust 802.1p/DSCP/IP Prec (ingress)	Exigido
36	Soporte de limitación de tráfico mediante lista de control de acceso (ACL) aplicable en los puertos fisicos o VLANs por:	
37	Filtros basados en direcciones MAC origen o destino	Exigido
38	Filtros basados en direcciones IP origen o destino	Exigido
39	Filtros basados en número de puerto TCP/UDP	Exigido
40	Cantidad de filtros de trafico (ACL) (mínimo)	1500
	Spanning Tree Protocol	
41	IEEE 802.1d.	Exigido
42	Rapid Spanning Tree IEEE 802.1w	Exigido
43	Multiple Spanning Tree Protocol IEEE 802.1s.	Exigido
	Soporte de ruteo layer 3 por medio de los siguientes protocolos :	
44	Rutas Estáticas	Exigido
45	Soporte maximo de rutas IPv4	512 prefijos ; 4096 rutas
46	Soporte de IEEE802.1ag Ethernet OAM connectivity fault management (CFM)	Exigido
47	Soporte de Ethernet ring protection switching (ERPS, G.8032/Y.1344)	Exigido
48	Soporte de TDR (Time Domain Reflectometry). Una tecnologia que permite el segumiento y senializacion de fallas en los cables o conectores de redes de computadoras. Los puertos deben ser capaces de generar un pulso electromagnético, cuando este pulso alcanza un obstáculo o el fin del cable se genera un eco que es traducido en la distancia a la falla .	Opcional
49	RIP v1/v2	Exigido
50	RIPng	Exigido
51	Soporte OSPF	Exigido

52	Soporte de Layer 2 protocol tunneling (L2PT)	Exigido
53	Soporte de ARP (numero de entradas)	1024
	Funcionalidades layer 2	
54	Soporte de direcciones MAC de red (mínimo)	15000
55	Soporte de tramas Jumbo	Exigido
56	Soporte de IEEE 802.1X para VLAN VoIP.	Exigido
57	Port-based VLAN	Exigido
58	MAC-based VLAN	Exigido
59	Soporte IEEE 802.1Q-in-Q: VLAN Stacking	Exigido
60	IEEE 802.1ak: Multiple VLAN Registration Protocol (MVRP)	Exigido
61	Compatible con Per-VLAN Spanning Tree Plus	Exigido
62	Soporte de interfaces RVI (Routed VLAN Interfaces)	Exigido
63	Capacidad de soportar definición de dominios de broadcast VLANs (Virtual LANs) en todos los puertos según IEEE 802.1 p/Q.	Exigido
64	Numero de VLANs configurables en el Virtual Chasis (mínimo)	4000
65	VLANS en equipo individual (mínimo)	4000
66	Posible rango de VLAN-ID para configurar	Entre 1 - 4000
67	Soporte de DHCP Relay y DHCP helper	Exigido
68	Soporte de DHCP Server sobre interfaces RVI	Exigido
69	Voice VLAN fallback	Exigido
	Multicast	
70	Soporte protocolo IGMP-Snooping	Exigido
71	Soporte PIM-SM, PIM-SSM, PIM-DM	Exigido
72	Soporte IGMP: v1, v2, v3	Exigido
	Administracion / Management	
73	Deberá soportar Simple Network Management Protocol versión SNMP v2c ,SNMP v3.	Exigido
74	Capacidad de proveer los bloques de información de management (MIBs) necesarios.	Exigido

75	Capacidad de Remote Monitoring (RMON), deberá soportar al menos cuatro (4) grupos (statistics, history, alarm, events).	Exigido
76	sFlow	Exigido
77	Soporte de registro remoto (SysLog).	Exigido
78	Soporte de traffic mirroring por puerto o por VLAN.	Exigido
79	Deberá soportar Network Timing Protocol (NTP).	Exigido
80	Creación de perfiles de administrador con facultadas especificas de modificar la configuración o solo acceder a vistas de la misma y listado de comandos disponibles para ejecutar por cada perfil	Exigido
81	Las passwords (claves) de administrador almacenadas localmente deben estar encriptadas usando hash MD5 o SHA1	Exigido
82	Soporte de MIB para la información de media attachment unit (MAU)	Exigido
83	Fuente para AC	Exigido
84	Accesorios necesarios para montar en racks estándar de 19.	Exigido
	Seguridad, mecanismos soportados	
85	Central Web authentication	Exigido
86	Deberá soportar autentificación 802.1X. para diferentes VLANs por puerto.	Exigido
87	Soporte de IEEE 802.1X con soporte de VLANs de invitados (Guest VLAN)	Exigido
88	MAC Radius Authentication con 802.1X	Exigido
89	Soporte de protocolo EAP-PAP para MAC RADIUS authentication	Exigido
90	Soporte de seguridad del puerto mediante filtrado por dirección MAC. En caso de violación del puerto deberá poder enviarse una alerta al administrador y deshabilitar el puerto.	Exigido
91	Soporte de limitación de direcciones MAC por puerto.	Exigido
92	Soporte de Persistent MAC learning o sticky MAC	Exigido
93	DHCP Snooping.	Exigido
94	Dynamic ARP inspection (DAI)	Exigido
95	Proxy ARP	Exigido
96	Static ARP support	Exigido
97	IP source guard	Exigido
98	Orden de autenticación flexible	Exigido

99	IPv6 Neighbor Discovery inspection	Exigido
	Servicio de configuración por medios seguros	
100	Soporte Telnet / Secure Shell (SSH) versión 2 para conexión remota vía interfaz línea de comando (CLI).	Exigido
101	Soporte vía Web con SSL. (HTTPS)	Exigido
102	Soporte de creación de Certificados locales para conexión HTTPs	Exigido
103	Almacenamiento de sistema operativo y configuración en memoria Flash reescribible. (mínimo)	1 GB
104	Roll-back a varias configuraciones anteriores almacenadas en el equipo (mínimo 3 configuraciones) o una configuración de rescate almacenada especialmente por el administrador	Exigido
105	Mecanismos de automatización mediante scripts o similares que permitan chequear el cumplimiento y administrar los cambios de configuraciones, aplicar configuraciones predefinidas, visualizar conjuntos de comandos para el diagnóstico, análisis y administración de eventos, y generar respuestas predefinidas a eventos.	Exigido
106	Configuración por medio de consola serial asincrónica. Proveer al menos cinco cables	Exigido
107	La unidad deberá ser entregada con 1 (uno) juego de manuales de configuración de hardware y software. Estos manuales podrán ser entregados como original en papel ó en CD-ROM.	Exigido
108	Equipos alimentados con 220 V - 50 Hz, monofásico con toma de 3 patas, sin necesidad de requerir un transformador adicional.	Exigido
	Troubleshooting	
109	Debugging: CLI via console, telnet, or SSH	Exigido
110	Diagnostics: Show and debug command statistics	Exigido
111	Traffic mirroring (port)	Exigido
112	Traffic mirroring (VLAN)	Exigido
113	ACL-based mirroring	Exigido
114	Mirroring destination ports per system	Exigido
115	LAG port monitoring	Exigido
116	Multiple destination ports monitored to 1 mirror (N:1)	Exigido
117	Maximum number of mirroring sessions	Exigido
118	Mirroring to remote destination (over L2)	Exigido
119	IP tools: Extended ping and trace	Exigido

	Alta disponibilidad	
120	Soporte de Link Aggregation	Exigido
121	802.3ad (LACP) support: Number of LAGs supported	128
122	Maximum number of ports per LAG:	8
	LAG sharing algorithm—Routed Multicast Traffic:	
123	Tagged ports support in LAG	Exigido
124	Uplink Failure Detection (UFD)	Exigido
125	Soporte para equipos con dos Routing engines, configurar al Routing engine de respaldo para asumir el rol de master sin causar interrupcion en el reenvio.	Exigido
126	Soporte VRRP (Virtual Router Redundancy Protocol)	Exigido
	Alimentación Eléctrica, Ventilación y dimensiones.	
127	Tensión de operación Fuente de Alimentación 100-120V / 200-240V auto detectable.	Exigido
128	Cumplimiento de ROHS, EMC certification, Safety certification, Manufacturing certification	Opcional
129	Temperatura de operación: 0°C a 45°C	Exigido
130	Humedad de operación: 10% a 85% de humedad relativa máxima, sin condensación.	Exigido
131	Montaje en rack de 19	Exigido
132	Cantidad de Unidad de Rack del Equipo	1U
133	MTBF (mínimo)	87.600 hs

LOTE N° 2 ADQUISICIÓN DE EQUIPOS DE SEGURIDAD FORTINET

ITEM N° 1 - SOLUCIÓN ANTISPAM Y SEGURIDAD PARA CORREO

Nro.	Descripción	Requerimiento mínimo exigido
1	Marca	indicar
2	Modelo	indicar
3	Procedencia	indicar

4	Cantidad	2 (dos)

	Requisitos Mínimos	REQUERIDO
5	Mínimo 4 interfaces RJ45 10/100/1000	REQUERIDO
6	Se deben poder configurar al menos 60 dominios de correo electrónico en la solución	REQUERIDO
7	La solución debe incluir al menos dos discos de 1 TB y debe soportar arreglos RAID 0 y RAID 1 mínimamente por software	REQUERIDO
8	La solución debe poder también tener la capacidad de ser configurada como servidor de correo electrónico, soportando un mínimo de 380 casillas de correo.	REQUERIDO
9	La solución debe soportar la configuración de al menos 200 políticas de remitentes por cada dominio.	REQUERIDO
10	La solución debe ser capaz de procesar un mínimo de 240.000 mensajes de correo electrónico por hora.	REQUERIDO
11	La solución debe ser capaz de procesar un mínimo de 180.000 mensajes de correo electrónico por hora con la funcionalidad de Anti-Spam activada.	REQUERIDO
12	La solución debe ser aprovisionada en formato de appliance físico.	REQUERIDO

	Implementación y Modos de Operación	REQUERIDO
13	Todas las funcionalidades deben ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo y por un periodo mínimo de 36 meses.	REQUERIDO
14	Solución debe basarse en "appliance" de proposito especifico (Fisico). No se tendrán en cuenta los equipos de uso general (PCs o servidores) en la que se puede instalar y / o ejecutar un sistema operativo regular, como Microsoft Windows, FreeBSD, Solaris de Sun o GNU / Linux.	REQUERIDO

15	La solución debe ser capaz de funcionar como un gateway SMTP para los servidores de correo existentes.	REQUERIDO
16	La solución debe ser capaz de actuar como gateway, en calidad de MTA (Mail Transfer Agent).	REQUERIDO
17	La solución debe ser capaz de funcionar de una manera transparente, actuando como un proxy transparente para el envío de mensajes a los servidores de correo protegidas.	REQUERIDO
18	Debe poder ser instalado en forma de proxy SMTP transparente, para el análisis de correo saliente, buscando evitar el reporte en Blacklist	REQUERIDO
19	La solución debe soportar su implementación en modo de servidor, operando como un servidor de correo MTA independiente con buzones para los usuarios. Debe ser capaz de almacenar localmente mensajes de correo electrónico para su entrega a los usuarios a través de correo Web, POP3 y / o IMAP.	REQUERIDO
20	Debe tener disponible un API basado en REST para fines de monitoreo, automatización y orquestación.	REQUERIDO
21	La solución debe ser licenciada sin importar el número de buzones que proteja. El licenciamiento es basado en el performance del hardware suministrado (correo por hora)	REQUERIDO
	Características Generales de Seguridad de Correo Electrónico	**REQUERIDO**
23	La solución debe soportar listas blancas (seguras) y negras por dirección de correo, por dominio y direcciones IP	REQUERIDO
24	La solución debe permitir la sobreescritura, la edición y personalización de los mensajes de notificación de antivirus.	REQUERIDO
25	La solución debe poder permitir aplicar políticas basadas en la dirección IP del remitente	REQUERIDO
26	La solución debe proporcionar soporte para múltiples dominios de correo electrónico.	REQUERIDO

27	La solución debe ser compatible con la implementación de políticas por destinatario, de dominio, del tráfico entrante o saliente.	REQUERIDO
28	La solución debe ser capaz de entregar el correo en función de los usuarios existentes en una base de LDAP.	REQUERIDO
29	La solución debe soportar cuarentena por usuario, permitiendo que cada usuario puede gestionar sus propios mensajes en cuarentena la eliminación o la liberación de los que no son spam, lo que reduce la responsabilidad del administrador y la posibilidad de bloquear el correo electrónico legítimo.	REQUERIDO
30	La solución debe ser capaz de programar el envío de informes de cuarentena.	REQUERIDO
31	La solución debe ser capaz de realizar el almacenamiento (o archivado) de correo electrónico, basado en políticas, por ejemplo, archivado de correos electrónicos basado en ciertos remitentes o si el correo electrónico contiene determinadas palabras.	REQUERIDO
32	La solución debe ser capaz de mantener la cola de correo en caso de fallo en la conexión de salida, retrasos o errores de entrega.	REQUERIDO
33	La solución debe ser capaz de realizar la autenticación SMTP a través de LDAP, RADIUS, POP3 o IMAP.	REQUERIDO
34	La solución debe ser capaz de mantener listas de reputación del remitente sobre la base de: número de virus enviado, la cantidad de correos electrónicos considerados correo no deseado, la cantidad de destinatarios equivocados.	REQUERIDO
35	La solución debe ser compatible con el enrutamiento en IPv4 y IPv6.	REQUERIDO
36	La solución debe permitir el almacenamiento de correo electrónico a nivel local o servidor remoto.	REQUERIDO
37	La solución debe tener características antispam y antivirus	REQUERIDO
38	La solución debe ser capaz de realizar la inspección del correo de Internet entrante y saliente.	REQUERIDO

39	La solución debe contar con un Wizard para el fácil y rápido aprovisionamiento de las configuraciones básicas del equipo y de los dominios a proteger	REQUERIDO
40	La solución debe proporcionar protección contra ataques de denegación de servicio, tales como Mail Bomb	REQUERIDO
41	La solución debe proporcionar un control DNS reverso para la protección contra los ataques spoofing.	REQUERIDO
	Funcionalidades de Anti-Spam	**REQUERIDO**
42	La solución se debe conectar en tiempo real con la base de datos del fabricante para descargar actualizaciones de Anti-Spam.	REQUERIDO
43	La solución puede detectar si el origen de una conexión es lícito basado en una base de datos de reputación de IPs suministrada por el fabricante.	REQUERIDO
44	La solución debe contar con mecanismos de detección de SPAM nuevo, mediante el análisis continuo de los correo recibidos y su posterior correlación con eventos ocurridos a nivel mundial, permitiendo así definir y detectar nuevas reglas de SPAM	REQUERIDO
45	La solución debe ser capaz de realizar análisis Heurístico y definir umbrales máximos de acuerdo al comportamiento del correo y así determinar si un correo es spam.	REQUERIDO
46	La solución debe ser capaz de realizar análisis Bayesiano para determinar si un correo es spam.	REQUERIDO
47	La solución debe ser capaz de detectar si el correo electrónico es un boletín de noticias (Newsletter).	REQUERIDO
48	La solución debe contar con técnica que detecten SPAM mediante el uso de Greylist, las cuales clasifican el correo con base en su compartimiento en el inicio de sesión, como bloquear todos los correos y permitir solo los reenvíos.	REQUERIDO
49	La solución debe ser capaz de realizar análisis sobre la base de palabras prohibidas (Banned Words).	REQUERIDO

50	La solución debe contar con Diccionarios predefinidos de palabras que pueden ser escaneados en el correo electrónico, además definir pesos a cada diccionario o palabra creada para definir si un correo es SPAM.	REQUERIDO
51	La solución permite crear lista blancas o negras de palabras.	REQUERIDO
52	La solución debe permitir la gestión del spam con la capacidad de aceptar, encaminar (Relay), rechazar (Reject), descartar (Discard), poner en cuarentena personal, sobre escribir el destinatario, Archivar, enviar copia oculta BCC, reenviar a otro Host, Insertar un TAG o un nuevo encabezado.	REQUERIDO
53	La solución debe ser capaz de realizar documentos de análisis de imagen y PDF identificando con base en esto si el correo es SPAM.	REQUERIDO
54	La solución debe ser capaz de soportar las listas negras de terceros tales como DNSBL y SURBL.	REQUERIDO
55	La solución permite identificar imágenes que hagan alusión a contenido SPAM. Debe soportar el análisis (al menos) de las siguientes extensiones GIF, JPEG, PNG.	REQUERIDO
	Manejo de Sesiones	**REQUERIDO**
56	La solución debe ser compatible con Sender Policy Framework (SPF).	REQUERIDO
57	La solución debe ser compatible con Domain Keys Identified Mail (DKIM).	REQUERIDO
58	La solución debe ser compatible con Domain Based Message Authentication (DMARC).	REQUERIDO
59	La solución debe identificar altos volúmenes de conexiones y aplicar limites basado en senders e Ips.	REQUERIDO
60	La solución debe ser capaz de realizar una inspección minuciosa de los encabezados de correo electrónico.	REQUERIDO
	Administración y Alta Disponibilidad (HA)	**REQUERIDO**

61	La solución debe permitir su configuración a través del acceso web (HTTP, HTTPS).	REQUERIDO
62	La solución debe ser capaz de permitir la creación de administradores únicos para la administración y configuración de la solución por dominio, siendo también posible restringir el acceso por dirección IP y la máscara de red de origen.	REQUERIDO
63	La solución debe ser capaz de proporcionar al menos dos niveles de gestión de acceso: lectura / escritura (Read/Write) o de sólo lectura (Read Only)	REQUERIDO
64	La solución debe permitir la creación de perfiles de configuración granular, donde cada perfil puede agregar características de configuración específicos, tales como anti-spam, anti-virus, autenticación, entre otros.	REQUERIDO
65	La solución debe permitir esquemas de alta disponibilidad, tanto Activo-Activo como Activo-Pasivo	REQUERIDO
66	Cuando la solución se implementa para alta disponibilidad debe ser capaz de controlar el estado del enlace.	REQUERIDO
67	Cuando la solución se implementa para alta disponibilidad, debe ser capaz de sincronizar los mensajes de e-mails en cuarentena.	REQUERIDO
68	Cuando la solución se implementa para alta disponibilidad activo / Pasivo debería ser posible sincronizar los mensajes de correo electrónico y configuraciones.	REQUERIDO
69	Cuando la solución se implementa para alta disponibilidad debe ser capaz de detectar y reportar el fallo de un dispositivo.	REQUERIDO
	Funcionalidades de Protección Anti-Malware	**REQUERIDO**
70	La solución debe ser capaz de filtrar y analizar los archivos adjuntos y el contenido del e-mail.	REQUERIDO
71	La solución debe ser capaz de ejecutar el análisis antivirus en archivos comprimidos como RAR, ARJ, LHA, ZIP y PKZIP.	REQUERIDO

72	La solución debe contar con una base de datos de malware suministrada por el fabricante, la cual puede ser actualizada recurrentemente.	REQUERIDO
73	Ante la detección de un malware, la solución puede ejecutar las siguientes acciones: reenviar el correo y el malware a una cuenta definida, reescribir el destinatario.	REQUERIDO
74	La solución debe tener la capacidad de realizar protección anti-malware basándose en analíticas de su propia plataforma de inteligencia de amenazas, y por lo tanto, permitir la identificación rápida de nuevas amenazas.	REQUERIDO
	Funcionalidades de DLP	**REQUERIDO**
75	También debe proporcionar una solución DLP para detectar la información sensible que puede estar llegando por e-mail.	REQUERIDO
76	La funcionalidad DLP debe permitir definir la información a detectar como palabras, frases y expresiones regulares.	REQUERIDO
77	La funcionalidad DLP debe tener una lista predefinida de tipos de información y diccionarios, tales como números de tarjetas de crédito y otros.	REQUERIDO
78	La funcionalidad DLP debe permitir la creación y almacenamiento de impresiones digitales (Fingerprint) de documentos.	REQUERIDO
79	La funcionalidad DLP para permitir la creación de filtros por tipos de archivos;	REQUERIDO
80	La funcionalidad DLP debe permitir la generación y almacenamiento de impresiones digitales (fingerprints) de los archivos adjuntos de correo electrónico.	REQUERIDO
81	La funcionalidad DLP debe permitir el almacenamiento de impresiones digitales (Fingerprints) de archivos antiguos y también para los nuevos archivos que se han actualizado.	REQUERIDO
	Encriptacion y Cifrado	**REQUERIDO**

82	Debe soportar cifrado de mensajes basado en identidad (IBE- Identity Based Encryption), de tal forma que el destinatario no requiera de un PSK o certificado previamente instalado para su descifrado	REQUERIDO
83	El cifrado de mensajes con IBE, debe soportar tanto el metodo push como pull, donde el mensaje cifrado estará almacenado en la plataforma de correo para su acceso remoto autenticado, o bien sea enviado como un adjunto al destinatario.	REQUERIDO
84	En ambos métodos de cifrado con IBE se debe contar con un registro del destinatario en la plataforma de correo, de tal forma que para ver los mensajes cifrados se requiera un proceso de autenticación.	REQUERIDO
85	Debe soportar cifrado de correo usando S/MIME	REQUERIDO
86	Debe soportar cifrado SMTPS	REQUERIDO
	Registros y Reportes	**REQUERIDO**
87	La solución debe ser capaz de almacenar los registros y eventos a nivel local y también enviarlos a servidores remotos (Syslog).	REQUERIDO
88	La solución debe permitir que se informe de la actividad, el análisis de los archivos de eventos (logs) y presentarlos en formato de tabla o gráfica.	REQUERIDO
89	La solución debe generar informes por demanda o programados a intervalos de tiempo específicos	REQUERIDO
90	La solución debe generar y enviar informes en formato PDF o HTML.	REQUERIDO
	RFCs	**REQUERIDO**
91	Debe soportar el RFC 1213 (Management Information Base for Network Management of TCP/IP-based Internets: MIB-II)	REQUERIDO
92	Debe soportar el RFC 1918 (Address Allocation for Private Internets)	REQUERIDO

93	Debe soportar el RFC 1985 (SMTP Service Extension for Remote Message Queue Starting)	REQUERIDO
94	Debe soportar el RFC 2034 (SMTP Service Extension for Returning Enhanced Error Codes)	REQUERIDO
95	Debe soportar el RFC 2045 (Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies)	REQUERIDO
96	Debe soportar el RFC 2505 (Anti-Spam Recommendations for SMTP MTAs)	REQUERIDO
97	Debe soportar el RFC 2634 (Enhanced Security Services for S/MIME)	REQUERIDO
98	Debe soportar el RFC 2920 (SMTP Service Extension for Command Pipelining)	REQUERIDO
99	Debe soportar el RFC 3207 (SMTP Service Extension for Secure SMTP over TLS)	REQUERIDO
100	Debe soportar el RFC 3461 (SMTP Service Extension for Delivery Status Notifications DSNs)	REQUERIDO
101	Debe soportar el RFC 3463 (Enhanced Mail System Status Codes)	REQUERIDO
102	Debe soportar el RFC 3464 (Extensible Message Format for Delivery Status Notifications)	REQUERIDO
103	Debe soportar el RFC 3635 (Definitions of Managed Objects for the Ethernet-like Interface Types)	REQUERIDO
104	Debe soportar el RFC 4954 (SMTP Service Extension for Authentication)	REQUERIDO
105	Debe soportar el RFC 5321 (SMTP)	REQUERIDO
106	Debe soportar el RFC 5322 (Internet Message Format)	REQUERIDO
107	Debe soportar el RFC 6376 (DomainKeys Identified Mail (DKIM) Signatures)	REQUERIDO

108	Debe soportar el RFC 6522 (Multipart/Report Content Type for the Reporting of Mail System Administrative Messages)	REQUERIDO
109	Debe soportar el RFC 6409 (Message Submission)	REQUERIDO
110	Debe soportar el RFC 7208 (Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail)	REQUERIDO
111	Debe soportar el RFC 2088 (IMAP4 Non-synchronizing Literals)	REQUERIDO
112	Debe soportar el RFC 2177 (IMAP4 Idle Command)	REQUERIDO
113	Debe soportar el RFC 2221 (Login Referrals)	REQUERIDO
114	Debe soportar el RFC 2342 (IMAP4 Namespace)	REQUERIDO
115	Debe soportar el RFC 2683 (IMAP4 Implementation Recommendations)	REQUERIDO
116	Debe soportar el RFC 2971 (IMAP4 ID Extension)	REQUERIDO
117	Debe soportar el RFC 3348 (IMAP4 Child Mailbox Extensión)	REQUERIDO
118	Debe soportar el RFC 3501 (IMAP4 rev1)	REQUERIDO
119	Debe soportar el RFC 3502 (IMAP Multiappend Extensión)	REQUERIDO
120	Debe soportar el RFC 3516 (IMAP4 Binary Content Extensión)	REQUERIDO
121	Debe soportar el RFC 3691 (Unselect Command)	REQUERIDO
122	Debe soportar el RFC 4315 (UIDPLUS Extension)	REQUERIDO
123	Debe soportar el RFC 4469 (Catenate Extension)	REQUERIDO
124	Debe soportar el RFC 4731 (Extension to SEARCH Command for Controlling What Kind of Information Is Returned)	REQUERIDO

125	Debe soportar el RFC 4959 (Extension for Simple Authentication and Security Layer (SASL) Initial Client Response)	REQUERIDO
126	Debe soportar el RFC 5032 (WITHIN Search Extensión)	REQUERIDO
127	Debe soportar el RFC 5161 (Enable Extensión)	REQUERIDO
128	Debe soportar el RFC 5182 (Extension for Referencing the Last SEARCH Result)	REQUERIDO
129	Debe soportar el RFC 5255 (IMAP Internationalization)	REQUERIDO
130	Debe soportar el RFC 5256 (Sort and Thread Extensions)	REQUERIDO
131	Debe soportar el RFC 5258 (List Command Extensions)	REQUERIDO
132	Debe soportar el RFC 5267 (Contexts for IMAP4)	REQUERIDO
133	Debe soportar el RFC 5819 (Extension for Returning STATUS Information in Extended LIST)	REQUERIDO
134	Debe soportar el RFC 6154 (LIST Extension for Special-Use Mailboxes)	REQUERIDO
135	Debe soportar el RFC 6851 (MOVE extensión)	REQUERIDO
136	Debe soportar el RFC 7162 (IMAP Extensions: Quick Flag Changes Resynchronization (CONDSTOR) and Quick Mailbox Resynchronization (QRESYNC))	REQUERIDO
137	Debe soportar el RFC 1939 (POP3)	REQUERIDO
138	Debe soportar el RFC 2449 (POP3 Extensión Mechanism)	REQUERIDO
139	Debe soportar el RFC 1155 (Structure and Identification of Management Information for TCP/IP-based Interface)	REQUERIDO
140	Debe soportar el RFC 1157 (SNMP v1)	REQUERIDO
141	Debe soportar el RFC 1213 (MIB 2)	REQUERIDO

142	Debe soportar el RFC 2578 (Structure of Management Information Version 2)	REQUERIDO
143	Debe soportar el RFC 2579 (Textual Conventions for SMIv2)	REQUERIDO
144	Debe soportar el RFC 2595 (Using TLS with IMAP, POP3 and ACAP)	REQUERIDO
145	Debe soportar el RFC 3410 (SNMP v3)	REQUERIDO
146	Debe soportar el RFC 3416 (SNMP v2)	REQUERIDO

ITEM N° 2 - CORTAFUEGOS DE APLICACIONES WEB

Nro.	Descripción	Requerimiento mínimo exigido
1	Marca	indicar
2	Modelo	indicar
3	Procedencia	indicar
4	Cantidad	2 (dos)
	E Especificaciones de Hardware y Rendimiento	
5	La solución debe de ser del tipo appliance físico	REQUERIDO
6	Throughput (HTTP) minimo de 240 Mbps	REQUERIDO
7	Cantidad de interfaces 1 Gbps (RJ45): mínimo 4	REQUERIDO
8	Cantidad de interfaces 1 Gbps (SFP): mínimo 4	REQUERIDO

9	Cada equipo (appliance físico) debe de tener un firmware específico destinado a la finalidad de Firewall de Aplicación Web (WAF Web Application Firewall), así como las licencias necesarias para su funcionamiento y protección de servidores y aplicaciones Web.	REQUERIDO
10	Tener puerto consola RS-232 o RJ45, para acceso a la interfaz de linea de comandos	REQUERIDO
11	Tener LEDs para la indicación del status y actividades de las interfaces	REQUERIDO
12	La solución debe permitir implementación en modo Proxy Transparente, Proxy Reverso y Sniffer	REQUERIDO
13	La solución debe de ser capaz de ser implementada con protocolo WCCP	REQUERIDO
14	Soportar VLANs del estándar IEEE 802.1q.	REQUERIDO
15	Debe de implementar el protocolo Link Aggregation Control Protocol (LACP) - IEEE 802.3ad	REQUERIDO
16	Soportar direccionamiento IPv4 y IPv6 en las interfaces físicas y virtuales (VLANs).	REQUERIDO
17	La solución debe de soportar y brindar cluster de alta disponibilidad entre dos equipos en modo Activo-Pasivo y Activo-Activo, de forma que el tráfico siga siendo procesado en caso de fallo del equipo principal.	REQUERIDO
18	La solución debe de soportar la sincronización de configuración entre dos appliances del mismo tipo, con el objetivo de operar en modo activo-activo, con la distribución de tráfico siendo realizada por balanceador de tráfico externo o por la propia solución.	REQUERIDO
19	La solución debe de soportar enrutamiento por política (policy route)	REQUERIDO
	Administración de la Solución	**REQUERIDO**

20	El firmware debe soportar interfaz gráfica web para la configuración de las funciones del sistema, utilizando navegadores disponibles gratuitamente y protocolo HTTPS, y también por CLI (interface de línea de comando), accediendo localmente al equipo por puerto de consola, o remotamente vía SSH.	REQUERIDO
21	Debe de soportar administración basada en interface web	REQUERIDO
22	Tener la función de auto-completar comandos en la CLI	REQUERIDO
23	Tener la función de auto-completar comandos en la CLI	REQUERIDO
24	Tener ayuda contextual en la CLI	REQUERIDO
25	La solución debe de tener un Dashboard con información sobre el sistema (información del cluster, hostname, número de serie, modo de operación, tiempo en servicio, versión de firmware)	REQUERIDO
26	Debe de ser posible visualizar a través de la interfaz gráfica de gestión la información de licencia, firmas y contrato de soporte	REQUERIDO
27	La solución ofertada deberá de tener acceso a la línea de comando CLI directamente a través de la interfaz gráfica de gestión (GUI)	REQUERIDO
28	Debe de proveer, en la interfaz de gestión, la siguiente información del sistema para cada equipo: consumo de CPU y estadísticas de conexión	REQUERIDO
29	Debe de ser posible visualizar en la interfaz de gestión la información de consumo de memoria	REQUERIDO
30	Debe de incluir una herramienta dentro de la interfaz gráfica de gestión (dashboard) que permita visualizar los últimos logs de ataques detectados/bloqueados	REQUERIDO
31	Debe proveer la siguiente información en la interfaz gráfica de gestión: estadísticas de throughput HTTP en tiempo real, estadísticas de eventos de ataques detectados/bloqueados, estadísticas de requisición HTTP en tiempo real y los últimos logs de eventos del sistema	REQUERIDO

32	Tener en la interfaz gráfica estadísticas de conexión concurrente y por segundo, de políticas de seguridad del sistema	REQUERIDO
33	Tener un dashboard de visualización con información de las interfaces de red del sistema	REQUERIDO
34	La configuración de administración de la solución debe permitir la utilización de perfiles	REQUERIDO
35	Debe de ser posible ejecutar y recuperar backup por la interfaz Web (GUI)	REQUERIDO
36	Debe de tener la opción de cifrar el backup utilizando contraseña	REQUERIDO
37	Debe de ser posible ejecutar y recuperar el backup utilizando FTP	REQUERIDO
38	Debe de ser posible ejecutar y recuperar el backup utilizando SFTP y TFTP	REQUERIDO
39	Debe ser posible probar una nueva versión de firmware en memoria RAM, sin instalar en disco, antes de aplicarla	REQUERIDO
40	Debe ser posible instalar un firmware alternativo en disco y arrancarlo en caso de fallo del firmware principal	REQUERIDO
41	Debe soportar los protocolos de monitoreo SNMP.	REQUERIDO
42	Debe ser capaz de realizar notificación de eventos de seguridad a través de e-mail, traps SNMP y Syslog	REQUERIDO
43	La solución deberá de soportar almacenar logs localmente en disco y en servidor externo vía protocolo SYSLOG	REQUERIDO
44	Debe tener la capacidad de almacenar los logs en appliance remoto	REQUERIDO
45	La solución debe tener datos analíticos conteniendo la localización geográfica de los clientes web	REQUERIDO

46	La solución debe tener datos analíticos, siendo posible visualizar el total de ataques y porcentaje de cada país de origen, el volumen total de tráfico en bytes y porcentaje de cada país de origen, y el total de accesos (hits) y porcentaje de cada país de origen	REQUERIDO
47	Debe tener la capacidad de generar reportes detallados basados en tráfico/acceso/actividades del usuario	REQUERIDO
48	Debe soportar RESTful API para gestión de la configuración	REQUERIDO
	Autenticación	**REQUERIDO**
49	Los usuarios deben de ser capaces de autenticarse a través del encabezado de autorización HTTP/HTTPS	REQUERIDO
50	Los usuarios deben de ser capaces de autenticarse a través de formularios HTML embebidos	REQUERIDO
51	La solución debe de ser capaz de autenticar los usuarios a través de certificados digitales personales	REQUERIDO
52	Debe tener base local para almacenamiento y autenticación de los usuarios	REQUERIDO
53	La solución debe tener la capacidad de autenticar usuarios en bases externas remotas LDAP, RADIUS y SAML	REQUERIDO
54	La solución debe de ser capaz de autenticar los usuarios en base remota vía NTLM	REQUERIDO
55	La solución debe de ser capaz de crear grupos de usuarios para configurar mecanismos de autenticación por grupos	REQUERIDO
	Regulaciones y Certificaciones	**REQUERIDO**
56	La solución debe de soportar el modelo de seguridad positiva definido por OWASP y proteger contra el Top 10 de ataques a aplicaciones definido por OWASP	REQUERIDO
57	El equipo debe de tener certificación FCC Class A part 15	REQUERIDO
58	El equipo debe de tener certificación VCCI	REQUERIDO

59	El equipo debe de tener certificación CE	REQUERIDO
60	El equipo debe de tener certificación UL/CB/cUL	REQUERIDO
	Funcionalidades de Firewall de Aplicaciones Web	**REQUERIDO**
61	Todas las funcionalidades deben ser ILIMITADO en cuanto a usuarios, conexiones, equipos que pasan a través de la solución, limitándola solamente por el desempeño del equipo y por un periodo mínimo de 36 meses.	REQUERIDO
62	Debe tener soporte nativo de HTTP/2	REQUERIDO
63	Debe soportar traducción de HTTP/2 a HTTP 1.1	REQUERIDO
64	Deberá soportar interoperabilidad con OpenAPI 3.0	REQUERIDO
65	Debe de ser capaz de identificar y bloquear ataques a través de una base de datos de firmas de virus y reputación IP, la cual se debe actualizar automáticamente y de manera periódica	REQUERIDO
66	La solución debe permitir elegir entre utilizar la base de datos completa o solamente la base de datos que contiene los últimos y más peligrosos virus	REQUERIDO
67	Deberá tener algoritmos para detección de amenazas avanzadas basados en aprendizaje de máquina con Inteligencia Artificial (AI) para detectar anomalías y aprender si se trata de ataques o no	REQUERIDO
68	Deberá minimizar la ocurrencia de Falsos Positivos y falsos negativos utilizando Inteligencia Artificial	REQUERIDO
69	Tener mecanismo de aprendizaje automático capaz de identificar todos los contenidos de la aplicación, incluyendo URLs, parámetros de URLs, campos de formularios y lo que se espera de cada campo	REQUERIDO
70	El perfil aprendido de forma automática debe de poder ser ajustado	REQUERIDO
71	Tener la capacidad de creación de firmas personalizadas de ataques	REQUERIDO

72	Tener la capacidad de protección contra ataques del tipo Adobe Flash binary (AMF) protocol.	REQUERIDO
73	Tener la capacidad de protección contra ataques del tipo Botnet	REQUERIDO
74	La solución debe tener funcionalidad de protección contra ataques como acceso por fuerza bruta	REQUERIDO
75	Debe soportar detección de ataques de Clickjacking	REQUERIDO
76	Debe soportar detección de ataques de alteración de cookie	REQUERIDO
77	Identificar y proteger contra ataques del tipo Cross Site Request Forgery (CSRF)	REQUERIDO
78	La solución debe tener funcionalidad de protección contra ataques como cross site scripting (XSS)	REQUERIDO
79	Debe tener protección contra ataques de Denial of Service (DoS);	REQUERIDO
80	Tener la capacidad de protección contra ataques del tipo HTTP header overflow	REQUERIDO
81	Tener la capacidad de protección contra ataques del tipo Local File inclusión (LFI)	REQUERIDO
82	Tener la capacidad de protección contra ataques del tipo Man-in-the-middle (MITM)	REQUERIDO
83	Tener la capacidad de protección contra ataques del tipo Remote File Inclusión (RFI)	REQUERIDO
84	Tener la capacidad de protección contra ataques del tipo Server Information Leakage	REQUERIDO
85	Protección contra envíos de comandos SQL ocultos en las requisiciones enviadas a la base de datos (SQL Injection);	REQUERIDO
86	Identificar y prevenir ataques del tipo Low-rate DoS	REQUERIDO

87	Prevención contra Slow POST attack	REQUERIDO
88	Proteger contra ataques Slowloris	REQUERIDO
89	Tener la capacidad de protección contra ataques del tipo SYN flood	REQUERIDO
90	Tener la capacidad de protección contra ataques del tipo Forms Tampering	REQUERIDO
91	La solución debe tener funcionalidad de protección contra ataques de manipulación de campos ocultos	REQUERIDO
92	Tener la capacidad de protección contra ataques del tipo Directory Traversal	REQUERIDO
93	Tener la capacidad de protección del tipo Access Rate Control	REQUERIDO
94	Identificar y proteger contra Zero Day Attacks	REQUERIDO
95	Tener la capacidad de configurar protección del tipo TCP SYN flood-style para prevención de DoS para cualquier política, a través de Syn Cookie y Half Open Threshold	REQUERIDO
96	Permitir configurar reglas de bloqueo a métodos HTTP no deseados	REQUERIDO
97	Permitir que se configuren reglas de límite de upload por tamaño del archivo	REQUERIDO
98	Debe permitir que el administrador bloquee el tráfico de entrada o salida en base a países, sin la necesidad de gestionar manualmente los rangos de dirección IP correspondientes a cada país	REQUERIDO
99	Debe soportar crear políticas de geo-localización, permitiendo que el tráfico de determinado país sea bloqueado	REQUERIDO
100	Permitir configurar listas de bloqueo y listas de confianza, basadas en dirección IP de origen	REQUERIDO

101	Permitir la liberación temporal o definitiva (white-list) de direcciones IP bloqueadas por tener originado ataques detectados por la solución	REQUERIDO
102	Debe permitir añadir, automáticamente o manualmente, en una lista de bloqueo, las direcciones IP de origen, según la base de IP Reputation	REQUERIDO
103	Tener la capacidad de prevención contra fuga de información (DLP), bloqueando la fuga de información del encabezado HTTP	REQUERIDO
104	Tener la funcionalidad de proteger el website contra acciones de defacement, con recuperación automática y rápida del website en caso de fallo	REQUERIDO
105	Tener la funcionalidad de antivírus integrada para inspección de tráfico y archivos, sin la necesidad de instalación de otro equipo	REQUERIDO
106	Tener la capacidad de investigar y analizar todo el tráfico HTTP para validar si cumple con el RFC del protocolo HTTP o si ha sufrido alguna alteración y debe ser bloqueado	REQUERIDO
107	La solución debe de ser capaz de funcionar como terminador de sesión SSL para aceleraración de tráfico	REQUERIDO
108	Para SSL/TLS offload soportar al menos TLS 1.0, 1.1, 1.2 y 1.3	REQUERIDO
109	La solución debe tener la capacidad de almacenar certificados digitales de CA's	REQUERIDO
110	La solución debe de ser capaz de generar CSR para ser firmado por una CA	REQUERIDO
111	La solución debe de ser capaz de chequear los certificados válidos y que no fueron revocados por una lista CRL	REQUERIDO
112	La solución debe contener las firmas de bots conocidos como link checkers, indexadores de web, search engines, spiders y web crawlers que puedan ser añadidos a los perfiles de control de acceso, así como resetear dichas conexiones	REQUERIDO

113	La solución debe de tener un sistema de bloqueo con base en la reputación de direcciones IP públicas conocidas. La lista de IPs con mala reputación debe de ser actualizado automáticamente.	REQUERIDO
114	La solución debe de ser capaz de limitar el total de conexiones permitidas hacia cada servidor real de un pool de servidores	REQUERIDO
115	La solución debe permitir la customización o reenvío de request y response HTTP en el Host, URL, Referer, Body y Location	REQUERIDO
116	La solución debe de tener la capacidad de definir restricción a determinados métodos HTTP	REQUERIDO
117	Permitir que se configuren firmas personalizadas de ataques y DLP, a través de expresiones regulares	REQUERIDO
118	La solución debe permitir ejecutar escaneo de vulnerabilidades o la integración con scanners de vulnerabilidades de terceros, tales como Acunetix, IBM AppScan, WhiteHat, entre otros	REQUERIDO
119	Debe permitir programar el escaneo de vulnerabilidades	REQUERIDO
120	La solución debe generar un reporte de análisis de vulnerabilidades y permitir su descarga	REQUERIDO
121	Soportar redirección y reescritura de request y response HTTP	REQUERIDO
122	Permitir redirección de request HTTP hacia HTTPS	REQUERIDO
123	Permitir reescribir la línea URL del encabezado de un request HTTP	REQUERIDO
124	Permitir reescribir el campo HOST del encabezado de un request HTTP	REQUERIDO
125	Permitir reescribir el campo REFERER del encabezado de un request HTTP	REQUERIDO
126	Permitir redirigir request hacia otro website	REQUERIDO

127	Permitir enviar respuesta HTTP 403 Forbidden para request HTTP	REQUERIDO
128	Permitir reescribir el parámetro LOCATION en el encabezado HTTP de una respuesta de redirección de un servidor web	REQUERIDO
129	Permitir reescribir el cuerpo ("body") de un response HTTP de un servidor web	REQUERIDO
130	Permitir añadir el campo X-Forwarded-For para identificación de la dirección IP real del cliente cuando se encuentra en modo proxy reverso	REQUERIDO
131	La solución debe de soportar reglas para definir si los request HTTP serán aceptados en función de la URL y origen del request y, si necesario, aplicar una tasa específica de velocidad (rate limit).	REQUERIDO
132	Tener capacidad de caching para acelerar la entrega de contenido web	REQUERIDO
133	Debe permitir al administrador crear nuevas firmas y/o cambiar las firmas pre existentes	REQUERIDO
	Funcionalidades de Balanceo de Carga	**REQUERIDO**
134	Permitir prueba de disponibilidad del servidor web a través del método HTTP	REQUERIDO
135	Permitir prueba de disponibilidad del servidor web a través del método HTTPS	REQUERIDO
136	En las pruebas de disponibilidad HTTP y HTTPS, permitir indicar la URL exacta a ser probada	REQUERIDO
137	En las pruebas de disponibilidad HTTP y HTTPS, permitir elegir entre los métodos HEAD, GET y POST	REQUERIDO
138	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Host"	REQUERIDO
139	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "URL"	REQUERIDO

140	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Parámetro HTTP"	REQUERIDO
141	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Referer"	REQUERIDO
142	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Dirección IP de Origen"	REQUERIDO
143	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Encabezado".	REQUERIDO
144	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Cookie"	REQUERIDO
145	Soportar ruteo de las requisiciones de los clientes web basado en contenido HTTP a través de "Valor del campo del Certificado X509"	REQUERIDO
146	Implementar Cache de Contenido para HTTP, permitiendo que objetos sean almacenados y request HTTP sean contestados directamente por la solución	REQUERIDO
147	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por dirección IP de origen	REQUERIDO
148	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por análisis de cualquier parámetro del header HTTP	REQUERIDO
149	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por análisis del parámetro URL	REQUERIDO
150	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por cookie método cookie insert y cookie rewrite	REQUERIDO

151	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por embedded cookie (cookie original seguido de porción aleatoria)	REQUERIDO
152	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en Reescritura del Cookie	REQUERIDO
153	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en Cookie Persistente	REQUERIDO
154	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en ASP Session ID	REQUERIDO
155	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en PHP Session ID	REQUERIDO
156	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia basada en JSP Session ID	REQUERIDO
157	La solución debe de ser capaz de balancear las nuevas sesiones, pero manteniendo sesiones existentes en un mismo servidor, implementando persistencia por SSL session ID	REQUERIDO

CONDICIONES Y ACUERDO DE NIVEL DE SERVICIO

El Proveedor se compromete a cumplir el siguiente Acuerdo de Nivel de Servicio, bajo los siguientes términos:

- Los plazos para atención a solicitudes de asistencia técnica se determinarán de acuerdo al grado de criticidad y conforme a la severidad de problemas. La definición respecto al nivel de criticidad será determinada exclusivamente por la convocante en la solicitud de soporte.
- En caso de alguna falla en un equipo o bien suministrado, que impida su correcto uso o funcionamiento, se deberá prever un tiempo máximo de respuesta de 2 (dos) horas a partir de la comunicación, por correo electrónico u otro medio, de la convocante al proveedor. En este periodo de tiempo, la empresa debe gestionar los recursos necesarios y empezar a trabajar en la solución del evento.
- En caso de que un equipo presente fallas y no pueda ser reparado se deberá proveer, en carácter temporal- uno igual o de mayores prestaciones hasta la devolución del equipo reparado; se deberán dejar en funcionamiento todos los servicios con todas las configuraciones respectivas. Este soporte es solicitado por el tiempo que dure la Garantía.
- Además, se deberá incluir la revisión, backup, actualización y verificación a pedido de la convocante, acerca del funcionamiento periódico de todo el Hardware/Software utilizados y los cambios de elementos/partes que así lo

requieran en el momento y hora definido por la convocante.
- Los servicios solicitados por parte de la convocante o que sean necesarios y que involucren a los bienes y servicios objeto de la presente licitación, deberán ser proveídos por los técnicos propuestos en la oferta y no podrán ser reemplazados sin el consentimiento de la convocante.

TIEMPO DE RESPUESTA A INCIDENTES QUE AFECTAN LA DISPONIBILIDAD DEL SERVICIO

La convocante indicará los servicios/sistemas que serán considerados como críticos y no críticos y que serán atendidos en los siguientes plazos:

- Tiempo de respuesta a servicios/sistemas críticos: 2 (dos) horas desde la comunicación del incidente.
- Tiempo de respuesta a servicios/sistemas no críticos: 4 (cuatro) horas desde la comunicación del incidente.

SITUACIÓN ACTUAL

El edificio de la Dirección General de los Registros Públicos, ubicada en las calles Avda. Eusebio Ayala c/ Capitán Román García, cuenta con un edificio de 6 (seis) pisos. En cada uno de ellos, los funcionarios cuentan con sus computadoras personales, impresoras y equipos multifunción, todos éstos conectados a la red interna, totalizando aproximadamente 500 puestos de trabajo, siendo los pisos más densamente poblados la Planta Baja, el Entrepiso y el Primer Piso.

En cada piso, se ubican uno o más gabinetes de comunicaciones (rack), así como varios switches por piso como se describe en la tabla más abajo. Cada uno de los pisos tiene montado y operativo -al menos- dos cables de fibra óptica multimodo de 6 pelos y cada piso cuenta con su correspondiente DIO (Distribuidor Interno Óptico), en su gabinete respectivo.

Piso	Descripción	Cantidad de Switches
1	Planta Baja	5
2	Entrepiso	4
3	Primer Piso	7
4	Segundo Piso	2
5	Tercer Piso	1
6	Cuarto Piso	1
TOTAL		**20**

Descripción de pisos y cantidad de switches por piso

Como se muestra en la tabla superior, todos los pisos cuentan con varios switches de acceso y al menos uno de ellos con interfaces de fibra óptica de corta distancia (SFP), que permiten la conexión de cada piso con el equipo concentrador (switch core), que se encuentra en la Planta Baja y que a su vez se conecta al Centro de Datos (datacenter) ubicado en el Entrepiso de la Institución, y en donde funcionan los servicios y sistemas accedidos por los funcionarios y clientes externos.

Identificación de la unidad solicitante y justificaciones

1. **Identificar el nombre, cargo y la dependencia de la Institución de quien solicita el llamado a ser publicado.**

Mgtr. Abg. y N.P Lourdes González, Directora General, Dirección General de los Registros Públicos.

2. **Justificar la necesidad que se pretende satisfacer mediante la contratación a ser realizada.**

Este llamado tiene como beneficiarios principales a los funcionarios de la DGRP y a los ciudadanos que utilizan los servicios. Los objetivos del proyecto son dobles: en primer lugar, proveer equipos de seguridad que reduzcan la posibilidad de intrusiones en los servidores de la Institución y protejan los datos almacenados. En segundo lugar, garantizar la disponibilidad de acceso a la red de datos mediante el reemplazo completo de los dispositivos de red que actualmente están fuera de soporte y han sido discontinuados por los fabricantes. Con estas medidas, se busca mejorar la seguridad y eficiencia en el manejo de la información de la institución, beneficiando tanto a los empleados como a la ciudadanía en general. Es importante mencionar que estos equipos cumpliran una tarea crítica en el funcionamiento de la infraestructura tecnológica de la DGRP, pues permitirán la interconexión de todos los equipos informáticos distribuidos en los pisos del edificio a los servidores del Centro de Datos, a los sistemas y carpetas compartidas, así como posibilitar el acceso a Internet, a la Red Metropolitana del Sector Público y a otras redes y servicios externos como aquellos que funcionan en la Corte Suprema de Justicia. Resulta vital contar con estos equipos considerando los servicios actualmente ofrecidos y los próximos a ofrecer y que serán accedidos vía Internet y/o intranet local, además de la necesidad del acceso a los servicios relacionados al sistema informático de Mesa de Entrada y Salida, que son requeridos para la entrada, consulta y expedición de documentos.

3. **Justificar la planificación. (si se trata de un llamado periódico o sucesivo, o si el mismo responde a una necesidad temporal).**

Responde a una necesidad crítica y urgente. El edificio de la DGRP, objeto de este servicio, alberga todas las transacciones registrales ligadas a la economía del País, así como las fincas matrices de titulación inmobiliaria de toda esta república, dependiente a un Poder del Estado, y en ella cumplen funciones de forma diaria las máximas autoridades de la Institución, y toda la estructura natural ligada a ese poder que compone el engranaje jurisdiccional y administrativo que hace al Servicio de Justicia, que se brinda a la ciudadanía en un Estado de Derecho.

Por tanto, se puede afirmar y confirmar la necesidad de contar con los bienes y servicios previamente indicados.

4. **Justificar las especificaciones técnicas establecidas.**

LOTE	ITEM	DESCRIPCIÓN
1	1	SWITCHES DE CORE
1	2	SWITCHES DE DATA CENTER
1	3	SWITCHES DE ACCESO
2	1	SOLUCIÓN ANTISPAM Y SEGURIDAD PARA CORREO **FORTINET FORTIMAIL**
2	2	CORTAFUEGOS DE APLICACIONES WEB **FORTINET FORTIWEB**

La elección de los equipos del Lote 2, FortiMail (Ítem 1) y FortiWeb (Ítem 2), de la marca Fortinet, se fundamenta en varias razones esenciales. Esto incluye la integración fluida con la infraestructura existente, respaldada por las destacadas características de seguridad y eficacia que caracterizan a la marca. Se busca establecer un sistema centralizado de administración y gestión de la seguridad de la información.

Es importante recordar que la CSJ recientemente adjudicó la compra de equipos de la marca Fortinet en el marco de la LICITACIÓN POR CONCURSO DE OFERTAS PAC N° 53/2022 "ADQUISICIÓN DE EQUIPOS DE CONMUTACIÓN, SEGURIDAD DE RED DE DATOS Y SOFTWARE DE REPORTES PLURIANUAL AD REFERÉNDUM S.B.E. ID N° 416.434. Para salvaguardar la inversión realizada y garantizar la cohesión en nuestro entorno de seguridad actual, la institución adquirió, a través de dicho proceso licitatorio, dispositivos que incluyen dos FortiSwitch 448E, dos FortiGate 200F y un FortiAnalyzer. Estos equipos han demostrado ser esenciales para la seguridad de la red de datos de la institución, proporcionando protección robusta contra amenazas y ofreciendo una plataforma eficiente para la monitorización y generación de reportes de seguridad.

La sinergia entre los dispositivos existentes -FortiGate 200F y FortiAnalyzer- y los que se pretenden adjudicar en este nuevo proceso licitatorio, que incluye dispositivos de seguridad de correo electrónico y de seguridad de aplicativos web, se basa en su capacidad para integrarse de manera nativa. Esto, junto con el uso de un esquema de interconexión propietario, facilita una colaboración estrecha y una respuesta coordinada a posibles amenazas. Esta interoperabilidad no solo simplifica la administración y la monitorización, sino que también optimiza la eficacia de las defensas de seguridad ante posibles amenazas y ataques.

El dispositivo FortiMail (Lote 1 - Ítem 1) desempeña un papel crucial como solución de seguridad de correo electrónico, esencial para prevenir amenazas dirigidas a través de este vector de ataque común. Al integrar FortiMail con la actual herramienta de monitoreo FortiAnalyzer, garantizamos una visibilidad completa y centralizada de las actividades relacionadas con el correo electrónico y su tráfico. Esto no solo facilita la detección temprana de posibles amenazas, sino que también mejora la capacidad de respuesta frente a incidentes.

Por otro lado, el dispositivo FortiWeb (Lote 1 - Ítem 2) juega un papel fundamental en la protección de las aplicaciones web contra ataques maliciosos. Su integración con el ecosistema Fortinet existente asegura una defensa coherente y unificada en todo el entorno tecnológico. Esto es esencial para salvaguardar los datos sensibles de la institución y mitigar eficazmente las amenazas dirigidas a través de aplicaciones web.

Además, la marca Fortinet ha ganado prestigio y una amplia participación en el mercado gracias a sus características de seguridad y precios altamente competitivos. La empresa ha establecido estándares elevados en términos de protección contra amenazas, rendimiento y escalabilidad. Esta combinación de seguridad de alta calidad y costos eficientes agrega un valor significativo a la inversión necesaria para contar con estos equipos y fortalecer la seguridad de la infraestructura de red de datos.

En el ámbito nacional, la presencia de varias empresas locales que comercializan equipos Fortinet destaca la disponibilidad y accesibilidad de estos productos. Empresas como Comtel, Netlogic, Technoma, ITseller, Teisa, Logicalis, Softshop, Telenet, Compusaver, Cidicom, entre otras, ofrecen opciones variadas, promoviendo un entorno propicio para obtener precios competitivos y condiciones favorables.

En resumen, la elección de los dispositivos FortiMail y FortiWeb de la marca Fortinet no solo se basa en la continuidad de la infraestructura existente y sus características técnicas, sino también en la posición destacada de la marca en el mercado, respaldada por una amplia red de distribuidores locales. Esto no solo asegura la disponibilidad de los productos, repuestos, soporte y asistencia técnica, sino que también promueve la competencia entre proveedores, beneficiando a la institución en términos económicos. No menos importante, contribuirá a la protección segura y centralizada del acceso a los valiosos activos de información de la institución, además de garantizar la disponibilidad continua de los servicios.

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 indicados a continuación:

- La entrega, instalación, configuración, puesta en marcha de los bienes y servicios, documentaciones técnicas y transferencia tecnológica será dentro de los **60 (sesenta) días hábiles** posteriores a la firma del contrato.
- Cronograma tentativo que indique las tareas, requerimientos, así como las fechas de instalación, configuración e implementación de los ítems en cuestión, previa validación y confirmación del cronograma por parte de los técnicos informáticos de la DGRP.
- Cronograma, contenido y fechas tentativas para la realización de la transferencia tecnológica de los ítems ofertados.

Todo esto, debe ser entregado, instalado, configurado, implementado y realizado en el edificio de la Dirección General de

los Registros Públicos, sito en la Avda. E. Ayala entre De La Victoria y Cap. Román García, o donde la convocante lo indique. El montaje y despliegue de equipos, cableados y lo que hiciera falta, se podrá realizar en los siguientes horarios:

- Ordinario: período normal de actividades de lunes a viernes de 07:00 hs. a 15:00 hs.
- Extraordinario: a pedido de la Institución (los días sábados, domingos y/o feriados y/o dentro de los días laborales ordinarios, pero fuera del periodo normal de actividades para las implementaciones que involucren corte en el servicio).

Las pruebas de funcionamiento se harán en horario a convenir con la Convocante, a fin de minimizar el impacto en el normal funcionamiento de los servicios de la Institución.

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:

- **El documento requerido para acreditar el cumplimiento contractual, será:** Acta de Recepción
- **Serán presentados:** 1 (un) Acta.
- **Frecuencia:** Conforme se establece en el Plan de Entregas establecido en el PBC.

PLANIFICACIÓN DE INDICADORES DE CUMPLIMIENTO

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA (se indica la fecha que debe presentar según el PBC)
ACTA DE RECEPCIÓN	*ACTA*	La entrega, instalación, configuración, puesta en marcha de los bienes y servicios, documentaciones técnicas y transferencia tecnológica será dentro de los **60 (sesenta) días hábiles** posteriores a la firma del contrato.

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

Criterios de Adjudicación

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

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

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

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

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

Notificaciones

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

1. Dentro de los cinco (5) días corridos de haberse resuelto la adjudicación, la convocante comunicará a través del Sistema de Información de Contrataciones Públicas, copia del informe de evaluación y del acto administrativo de adjudicación, los cuales serán puestos a disposición pública en el referido sistema. Adicionalmente el sistema generará una notificación a los oferentes por los medios remotos de comunicación electrónica pertinentes, la cual será reglamentada por la DNCP.

2. En sustitución de la notificación a través del Sistema de Información de Contrataciones Públicas, las convocantes podrán dar a conocer la adjudicación por cédula de notificación a cada uno de los oferentes, acompañados de la copia íntegra del acto administrativo y del informe de evaluación. La no entrega del informe en ocasión de la notificación, suspende el plazo para formular protestas hasta tanto la convocante haga entrega de dicha copia al oferente solicitante.

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

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

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

Audiencia Informativa

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

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

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

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

Documentación requerida para la firma del contrato

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

1. Personas Físicas / Jurídicas
• Certificado de no encontrarse en quiebra o en convocatoria de acreedores expedido por la Dirección General de Registros Públicos;
• Certificado de no hallarse en interdicción judicial expedido por la Dirección General de Registros Públicos;
• Constancia de no adeudar aporte obrero patronal expedida por el Instituto de Previsión Social;

• Certificado laboral vigente expedido por la Dirección de Obrero Patronal dependiente del Viceministerio de Trabajo, siempre que el sujeto esté obligado a contar con el mismo, de conformidad a la reglamentación pertinente - CPS;
• En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para asumir todas las obligaciones emergentes del contrato hasta su terminación;
• Certificado de cumplimiento tributario vigente a la firma del contrato.
2. Documentos. Consorcios
• Cada integrante del consorcio que sea una persona física o jurídica deberá presentar los documentos requeridos para oferentes individuales especificados en los apartados precedentes.
• Original o fotocopia del consorcio constituido.
• Documentos que acrediten las facultades del firmante del contrato para comprometer solidariamente al consorcio.
• En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para asumir todas las obligaciones emergentes del contrato hasta su terminación.

CONDICIONES CONTRACTUALES

Esta sección constituye las condiciones contactuales 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 las mismas no está de acuerdo con los Incoterms, 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.

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;
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: **NO APLICA.**

Formulario de Informe de Servicios Personales (FIS): **NO APLICA.**

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 de los servicios facturados se reajustará durante el periodo de ejecución del contrato, a partir de una variación significativa de precios ocurrida en la economía nacional, que será medida a través del Índice de Precios al Consumo, publicado por el Banco Central del Paraguay, en una relación porcentual igual o mayor al 15% (quince por ciento) del mencionado Índice acumulado a partir de la fecha de presentación de la Oferta.

Los ajustes deberán corresponder al periodo o mes de prestación de servicios y aplicados sobre el importe facturado y presentado para su pago.

El precio del contrato será reajustable, conforme a la siguiente fórmula:

$$A = \frac{P \times I.I.B.C.P}{15\%}$$

Dónde:

A= Precio ajustado de los servicios facturados.
P= Precio facturado de los servicios ofertados.
I.I.B.C.P. = Índice de Inflación emitido por el Banco Central del Paraguay.
15% (quince por ciento) = Mínimo necesario para reajuste del precio.

No se reconocerá reajuste de precios si el Proveedor se encuentra atrasado respecto a la prestación de los servicios o la Contratante haya podido constatar fehacientemente que el Proveedor se encuentra en incumplimiento de las obligaciones patronales de seguridad social.

Porcentaje de multas

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

0,50 %

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

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

Tasa de interés por Mora

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

0,01

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 regirán 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 regirán atendiendo a la reglamentación vigente.

3. La celebración de un Convenio Modificatorio conforme a las reglas establecidas en el artículo N° 63 de la Ley 2051/2003, que constituyan condiciones de agravación del riesgo cuando la Garantía de Cumplimiento de Contrato sea formalizada a través de póliza de caución, obliga al proveedor a informar a la compañía aseguradora sobre las modificaciones a ser realizadas y en su caso, presentar ante la contratante los endosos por ajustes que se realicen a la póliza original en razón al convenio celebrado con la contratante.

Limitación de responsabilidad

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

Responsabilidad del proveedor

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

Fuerza mayor

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

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

Causales de terminación del contrato

1. Terminación por Incumplimiento

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

i. Si el proveedor no entrega parte o ninguno de los bienes dentro del período establecido en el contrato, o dentro de alguna prórroga otorgada por la contratante; o

ii. Si el proveedor no cumple con cualquier otra obligación en virtud del contrato; o

iii. Si el proveedor, a juicio de la contratante, durante el proceso de licitación o de ejecución del contrato, ha participado en actos de fraude y corrupción;

iv. Cuando las multas por atraso superen el monto de la Garantía de Cumplimiento de Contrato;

v. Por suspensión de los trabajos, imputable al proveedor o al contratista, por más de sesenta días calendarios, sin que medie fuerza mayor o caso fortuito;

vi. En los demás casos previstos en este apartado.

2. Terminación por Insolvencia o quiebra

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

3. Terminación por conveniencia

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

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

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

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

Otras causales de terminación del contrato

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

No Aplica

Resolución de Conflictos a través del Arbitraje

Las partes se someterán a Arbitraje:

No

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

Fraude y Corrupción

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

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

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

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

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

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

Fraude y corrupción comprenden actos como:

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

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

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

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

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

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

MODELO DE CONTRATO

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

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

FORMULARIOS

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

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