

**PLIEGO DE BASES Y CONDICIONES**

---

Convocante:

**Ministerio de Salud Pública y Bienestar Social (MSPBS)**  
**Dirección Nacional de Vigilancia Sanitaria**

Nombre de la Licitación:

**ADQUISICIÓN DE INFRAESTRUCTURA  
TECNOLÓGICA PARA LA DNVS**

(versión 3)

ID de Licitación:

**398093**



Modalidad:

**Licitación Pública Nacional**

Publicado el:

**28/09/2021**

*"Pliego para la Adquisición de Bienes - Convencional"*  
*Versión 4*

## RESUMEN DEL LLAMADO

### Datos de la Convocatoria

ID de Licitación:	398093	Nombre de la Licitación:	Adquisición de infraestructura tecnológica para la DNVS
Convocante:	Ministerio de Salud Pública y Bienestar Social (MSPBS)	Categoría:	24 - Equipos, accesorios y programas computacionales, de oficina, educativos, de imprenta, de comunicación y señalamiento
Unidad de Contratación:	Dirección Nacional de Vigilancia Sanitaria	Tipo de Procedimiento:	LPN - Licitación Pública Nacional

### Etapas y Plazos

Lugar para Realizar Consultas:	Dpto. de SUOC - 4° Piso (Iturbe 883 casi Manuel Domínguez)	Fecha Límite de Consultas:	15/09/2021 12:00
Lugar de Entrega de Ofertas:	Dpto. de SUOC - 4° Piso (Iturbe 883 casi Manuel Domínguez)	Fecha de Entrega de Ofertas:	22/10/2021 09:30
Lugar de Apertura de Ofertas:	Dpto. de SUOC - 4° Piso (Iturbe 883 casi Manuel Domínguez)	Fecha de Apertura de Ofertas:	22/10/2021 10:00

### Adjudicación y Contrato

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

### Datos del Contacto

Nombre:	Claudia María Ojeda Rojas	Cargo:	Jefa del Dpto. de SUOC
Teléfono:	449944	Correo Electrónico:	subuoc.dnvs@mspbs.gov.py

# ADENDA

## Adenda

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

### **ADENDA N° 02/2021**

**LICITACION PUBLICA NACIONAL N° 01//2021 ADQUISICION DE INFRAESTRUCTURA TECNOLOGICA PARA LA DNVS ID N° 398.093.-**

Asunción, 24 de setiembre de 2021.

Se comunica al oferente que la convocante ha realizado la modificación en el Sistema de Información de Contrataciones Públicas (SICP), consistente en la fecha de entrega de sobres y apertura de ofertas.

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

# DATOS DE LA LICITACIÓN

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

## Contratación Pública Sostenibles - CPS

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

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

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

Criterios sociales y económicos:

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

Criterios ambientales:

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

Conducta empresarial responsable:

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

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

## **Difusión de los documentos de la licitación**

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

## **Aclaración de los documentos de la licitación**

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

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

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

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

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

## **Documentos de la oferta**

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

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

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

## **Oferentes en consorcio**

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

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

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

## **Aclaración de las ofertas**

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

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

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

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

## **Disconformidad, errores y omisiones**

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

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

Con la condición de que la oferta cumpla sustancialmente con los Documentos de la Licitación, la Convocante corregirá errores aritméticos de la siguiente manera y notificará 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 unitario y el precio total será corregido.
2. Si hay un error en un total que corresponde a la suma o resta de subtotales, los subtotales prevalecerán y se corregirá el total
3. En caso de que el oferente haya cotizado su precio en guaraníes con décimos y céntimos, la convocante procederá a realizar el redondeo hacia abajo.
4. Si hay una discrepancia entre palabras y cifras, prevalecerá el monto expresado en palabras a menos que la cantidad expresada en palabras corresponda a un error aritmético, en cuyo caso prevalecerán las cantidades en cifras de conformidad con los párrafos (1) y (2) mencionados.

## **Idioma de la oferta**

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

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

traducción:

*En cuanto a los documentos complementarios y textos impresos que formen parte de la oferta, estos se podrán presentar en el idioma de origen del documento, diferente al castellano, siempre que se presenten acompañados de una traducción fidedigna al idioma castellano, realizada por traductor matriculado. Se citan en forma enunciativa y no limitativa los siguientes textos complementarios: catálogos, anexos técnicos, folletos. Para efectos de la interpretación de la oferta, prevalecerá la traducción. Se encuentran exceptuados los documentos complementarios y textos impresos que se encuentren en idioma inglés, los cuales no requerirán traducción fidedigna al idioma castellano.*

## **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: Tres días hábiles antes de la fecha tope de la Consulta

lugar: Edificio de la DNVS Iturbe 883 c/ Manuel Domínguez

hora: 09:00 a 15:00 hs.

procedimiento: Visita Técnica

Nombre del funcionario responsable de guiar la visita: Ing. Marcos León y/o Lic. Waldir Torres, Dpto. de Informática.

participación Obligatoria: SI

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 ítems, el oferente deberá de presentar el documento emitido por el fabricante, que acredite fehacientemente que el mismo es Representante Oficial y/o Distribuidor Oficial por el Fabricante para el Paraguay de los equipos, y que el mismo se encuentra autorizado para prestar el servicio técnico y el cambio de partes por garantía para la región, ya sea mediante fotocopia simple del documento emitido por la firma autorizante o mediante de la presentación del Formulario.

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.

---

## **Ofertas Alternativas**

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

No Aplica

## **Copias de la oferta - CPS**

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

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

Cantidad de copias requeridas:

2 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:

90

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

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

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

## **Garantías: instrumentación, plazos y ejecución.**

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

## **Periodo de Validez de la Garantía de Mantenimiento de Oferta**

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

120

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

---

## **Porcentaje de Garantía de Fiel Cumplimiento de Contrato**

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

10,00 %

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

---

## **Periodo de validez de la Garantía de Cumplimiento de Contrato**

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

El mismo tendrá vigencia de 30 (treinta) días posteriores a la fecha en que el proveedor haya cumplido con todas las obligaciones contractuales.

---

## **Periodo de validez de la Garantía de los bienes**

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

Garantía escrita de 3 (tres) años para todos los ítems.

---

## **Tiempo de funcionamiento de los bienes**

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

El oferente deberá de asegurar la comercialización de repuestos para los equipos /o sistemas proveídos como mínimo durante los dos años posteriores al vencimiento del plazo de soporte técnico y garantía del fabricante establecido en el punto anterior.

---

## **Plazo de reposición de bienes**

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

5 (cinco) días, a partir de la recepción de la nota de reclamo a ser emitida por el Administrador del Contrato

El proveedor garantiza que todos los bienes suministrados están libres de defectos derivados de actos y omisiones que este hubiera incurrido, o derivados del diseño, materiales o manufactura, durante el uso normal de los bienes en las condiciones que imperen en la República del Paraguay.

1. La Contratante comunicará al proveedor la naturaleza de los defectos y proporcionará toda evidencia disponible, inmediatamente después de haberlos descubierto. La contratante otorgará al proveedor facilidades razonables para inspeccionar tales defectos.

Tan pronto reciba ésta comunicación, y dentro del plazo establecido en este apartado, deberá reparar o reemplazar los bienes defectuosos, o sus partes sin ningún costo para la contratante.

2. Si el proveedor después de haber sido notificado, no cumple dentro del plazo establecido, la contratante, procederá a tomar medidas necesarias para remediar la situación, por cuenta y riesgo del proveedor y sin perjuicio de otros derechos que la contratante pueda ejercer contra el proveedor en virtud del contrato.

---

## **Cobertura de Seguro de los bienes**

La cobertura de seguro requerida a los bienes será:

No Aplica

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

---

## **Sistema de presentación de ofertas**

El Sistema de presentación de ofertas para esta licitación será:

Un sobre

Los sobres deberán:

1. Indicar el nombre y la dirección del Oferente;
2. Estar dirigidos a la Convocante;
3. Llevar la identificación específica del proceso de licitación indicado en el SICP; y
4. Llevar una advertencia de no abrir antes de la hora y fecha de apertura de ofertas.
5. Identificar si se trata de un sobre técnico o económico.

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

## Plazo para presentar las ofertas

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

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

Cuando la presentación de 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 courier o entregadas personalmente, los sobres marcados como:

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

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

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

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

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

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

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

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

9. En el sistema de doble sobre, el acta de apertura técnica deberá ser comunicada al SICP, para su difusión, dentro de los dos (02) días hábiles de la realización del acto de apertura, se procederá de igual manera una vez finalizado el acto de apertura económico

# REQUISITOS DE CALIFICACIÓN Y CRITERIOS DE EVALUACIÓN

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

## Condición de Participación

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

## Requisitos de Calificación

### Capacidad Legal

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

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

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

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

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

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



## **Análisis de precios ofertados**

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

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

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

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

## **Certificado de Producto y Empleo Nacional - CPS**

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

La falta del CPEN no será motivo de descalificación de la oferta, sin embargo, el oferente no podrá acogerse al beneficio.

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

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

a) Consorcios:

a.1. Provisión de Bienes

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

## **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

<p>1. Formulario de Oferta (*)</p> <p>[El formulario de oferta y lista de precios, generados electrónicamente a través del SICP, deben ser completados y firmados por el oferente.]</p>
<p>2. Garantía de Mantenimiento de Oferta (*)</p> <p>La garantía de mantenimiento de oferta debe ser extendida, bajo la forma de una garantía bancaria o póliza de seguro de caución.</p>
<p>3. Certificado de Cumplimiento con la Seguridad Social. (**)</p>
<p>4. Certificado de Producto y Empleo Nacional, emitido por el MIC, en caso de contar. (**)</p>
<p>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. (**)</p>
<p>6. Declaración Jurada de Declaración de Miembros, de conformidad con el formulario estándar Sección Formularios (**)</p>
<p>7. Certificado de Cumplimiento Tributario (**)</p>
<p>8. Patente Comercial del municipio en donde esté asentado el establecimiento principal del oferente. (**)</p>
<p>9. Documentos legales</p>
<p>9.1. Oferentes Individuales. Personas Físicas.</p>
<ul style="list-style-type: none"><li>• Fotocopia simple de la Cédula de Identidad del firmante de la oferta. (*)</li></ul>
<ul style="list-style-type: none"><li>• Constancia de inscripción en el Registro Único de Contribuyentes - RUC. (*)</li></ul>
<ul style="list-style-type: none"><li>• 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. (*)</li></ul>
<p>9.2. Oferentes Individuales. Personas Jurídicas.</p>

<ul style="list-style-type: none"> <li>• 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 inscritos en la Sección Personas Jurídicas de la Dirección de Registros Públicos. (*)</li> </ul>
<ul style="list-style-type: none"> <li>• 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.</li> </ul>
<ul style="list-style-type: none"> <li>• 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. (*)</li> </ul>
9.3. Oferentes en Consorcio.
<p>1. Cada integrante del consorcio que sea una persona física domiciliada en la República del Paraguay deberá presentar los documentos requeridos para Oferentes Individuales especificados en el apartado Oferentes individuales. Personas Físicas. Cada integrante del consorcio que sea una persona jurídica domiciliada en Paraguay deberá presentar los documentos requeridos para Oferentes Individuales Personas Jurídicas. (*)</p>
<p>2. Original o fotocopia del consorcio constituido o del acuerdo de intención de constituir el consorcio por escritura pública en caso de resultar adjudicados y antes de la firma del contrato. Las formalidades de los acuerdos de intención y de los consorcios serán determinadas por la Dirección Nacional de Contrataciones Públicas (DNCP). (*)</p>
<p>3. Fotocopia simple de los documentos que acrediten las facultades de los firmantes del acuerdo de intención de consorciarse. Estos documentos pueden consistir en (*):</p> <ul style="list-style-type: none"> <li>• Un poder suficiente otorgado por escritura pública por cada miembro del consorcio (no es necesario que esté inscripto en el Registro de Poderes); o</li> <li>• 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.</li> </ul>
<p>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 (*):</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• 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.</li> </ul>

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

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

## Capacidad Financiera

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

a) contribuyente de IRACIS/IRE.

Deberán cumplir con el siguiente parámetro:

**a. Ratio de Liquidez:** activo corriente / pasivo corriente

Deberá ser igual o mayor que 1, en promedio, en los tres últimos años 2018, 2019, 2020

**b. Endeudamiento:** pasivo total / activo total

No deberá ser mayor a 0,80 en promedio, en los tres últimos años 2018, 2019, 2020

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

b) contribuyentes de IRPC/IRE SIMPLE

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales requeridos. 2018, 2019, 2020

c) contribuyentes de IRP

Deberán cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

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

d) contribuyentes de exclusivamente IVA General

Deberá cumplir el siguiente parámetro:

Eficiencia: (Ingreso/Egreso).

Deberá ser igual o mayor que 1, el promedio, de los ejercicios fiscales 2018, 2019, 2020

Contribuyente IRACIS (últimos 2018, 2019, 2020).

El promedio en los en los tres últimos años 2017,2018,2019, no deberá ser negativo.

Los oferentes con menos de tres años de antigüedad, podrán presentar sus balances Generales y estados financieros desde su existencia como empresa. (Para los consorcios, todos los integrantes de consorcio deberán cumplir con los criterios de capacidad financiera)

Observación: para hallar el promedio de los 3 años se calculará el índice de cada año y luego se sumarán estos índices y se dividirá entre la cantidad de años. En caso de empresas que tengan menos años de antigüedad, el promedio se realizará teniendo en cuenta la cantidad de años de existencia. En todos los casos se utilizarán dos decimales.

## Requisitos documentales para la evaluación de la capacidad financiera

a. Copia de Balance General y Estado de Resultados año 2018, 2019, 2020
b. Formulario 106-Renta, correspondiente a los ejercicios fiscales 2018-2019. Y 501 DEL EJERCICIO FISCAL 2020 PARA CONTRIBUYENTE IRE SIMPLE.
c. Formulario 120-Iva GENERAL DE LOS ULTIMOS 6 MESES

d. Formulario 104-Renta Personal correspondiente a los ejercicios fiscales 2018, 2019 Y FORMULARIO 515 PARA 2020.

## Experiencia requerida

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

Demostrar la experiencia en la **provisión y puesta en marcha de equipos de cómputo integrado de alta escalabilidad del tipo Hiperconvergente** con facturaciones de venta y/o recepciones finales por un monto equivalente al **50 %** como mínimo del monto total ofertado en la presente licitación, de los: **03 (tres) años. (2018, 2019 y 2020).**

## Requisitos documentales para la evaluación de la experiencia

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

## Capacidad Técnica

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

1. Fotocopia simple de Estatuto de Constitución y/o Constancia de RUC que demuestren una antigüedad mínima de 3 (tres) años de existencia legal (inclusive para firmas unipersonales).
2. Folletos, catálogos y/o impresos descriptivos de los sistemas y/o equipos ofertados, incluyendo el modelo exacto a ser ofertado con los vínculos (links/URLs) oficiales del fabricante, en donde se pueda certificar las especificaciones técnicas.
3. Detalle de las especificaciones técnicas, en el cual se incluyan las descripciones y demás requisitos exigidos en las ESPECIFICACIONES TECNICAS Y SUMINISTROS REQUERIDOS.
4. Garantía de buen funcionamiento y calidad de los sistemas y/o equipos ofertados, formalizada mediante una Carta en carácter de Declaración Jurada a nombre de la Convocante, por el plazo de 3 (tres) años para todos los ítems; a partir de la fecha de emisión de la Recepción Definitiva. Durante ese periodo, correrá a su cargo, por cuenta propia y sin costo para la Convocante, las reposiciones, sustituciones, reparaciones y/o modificaciones que correspondan, cuando se observasen fallas y/o deficiencias, por causas que le fueran imputables.
5. Nota en carácter de declaración jurada por la cual el Oferente se compromete a otorgar el Soporte Técnico de las soluciones y/o equipos ofertados (hardware y software), el servicio de actualizaciones

del software para los mismos, así como el escalamiento de soporte técnico al fabricante y apertura de casos, de conformidad a lo dispuesto en la ESPECIFICACIONES TECNICAS Y SUMINISTROS REQUERIDOS, por el plazo de 3 (tres) años para todos los ítems solicitados; a partir de la fecha efectiva de entrega de los bienes. El primer contacto de soporte deberá ser a través de la empresa oferente. Si el caso amerita la convocante puede decidir y tener la libertad de solicitar soporte exclusivamente de cada marca ofertada y de manera independiente. No será aceptado soporte unificados por el fabricante de hardware y/o software.

6. Documento emitido por el Fabricante, por el cual el mismo otorga garantía respecto a los equipos, para reemplazo de los mismos por defectos de fabricación (no se aceptarán reparaciones), como mínimo por el plazo de 3 (tres) años de cobertura para todos los ítems; a partir de la fecha de la emisión de la Recepción Definitiva.
7. Nota en carácter de declaración jurada por la cual el Oferente manifieste contar con el personal técnico certificado para la instalación y configuración de la solución de Hiperconvergencia, la prestación de servicios de implementación y soporte técnico.
8. Fotocopia simple de la documentación requerida con relación al personal propuesto, conforme se detalla a continuación:
  - a. Al menos 2 (dos) técnicos con certificación del fabricante de la solución de Hiperconvergencia.
  - b. Al menos 1 (uno) técnico con certificación de nivel experto del fabricante del Switch.
  - c. Al menos 1 (uno) técnicos con certificación de nivel profesional del fabricante del Switch.
  - d. Al menos 2 (dos) técnicos con certificación del fabricante de la solución de Seguridad (NGFW).
  - e. Al menos 1 (uno) Profesional con certificación ITIL vigente.
  - f. Todos los técnicos deberán ser funcionarios de carácter permanente del Oferente y residente en nuestro país al momento de la presentación de su propuesta contando con una antigüedad laboral en dicha empresa no menor a 1 un año que será demostrada a través de la planilla de IPS, de los últimos 12 meses, o contrato de trabajo vinculante al oferente.

Adicionalmente se requerirá 2 (dos) técnicos o personal responsable del Oferente que realizará la integración de los equipos ofertados con la infraestructura tecnológica existente en la DNVS, debiendo presentar:

- a. Certificado Citrix / Nutanix
- b. Planilla mensual de aporte obrero patronal del Instituto de Previsión Social, cuya presentación fuera exigible a la fecha de apertura de ofertas, en la cual se demuestre la antigüedad mínima del personal de 1 (un) año con relación a la fecha de apertura de ofertas.

9. Listado completo de equipos y modelos, diagrama físico, velocidad y tipo de conexiones físicas, detalles del contenido y espacio en U (unidades de rack) para el rack. Además, para los software y licencias se deberá presentar modelos, detalles de funcionalidad incluidas y versiones.

## Requisito documental para evaluar la capacidad técnica

a. <i>Fotocopia simple de Estatuto de Constitución y/o Constancia de RUC</i>
b. <i>Folleto, catálogos y/o impresos descriptivos de los sistemas y/o equipos ofertados</i>
c. <i>Listado de las especificaciones técnicas según requisitos exigidos en la ESPECIFICACIONES TECNICAS Y SUMINISTROS REQUERIDOS</i>
d. <i>Declaración Jurada a nombre de la Convocante de la Garantía de buen funcionamiento y calidad de los sistemas y/o equipos ofertados.</i>
e. <i>Declaración jurada por la cual el Oferente se obliga a otorgar el Soporte Técnico</i>

f. <i>Carta del Fabricante, por el cual el mismo otorga garantía respecto a los equipos</i>
g. <i>Declaración jurada por la cual el Oferente manifieste contar con el personal técnico especializado</i>
h. <i>Certificado del fabricante de la solución de Hiperconvergencia</i>
i. <i>Certificado de nivel profesional del fabricante del Switch</i>
j. <i>Certificado del fabricante de la solución de Seguridad (NGFW)</i>
k. <i>Certificado ITIL vigente</i>
ax. <i>Documento vigente emitido por el fabricante que acredite que los mismos se encuentran certificados para la instalación y puesta en marcha de los bienes ofertados</i>
all. <i>Planilla mensual de aporte obrero patronal del Instituto de Previsión Social</i>
n. <i>Certificado Citrix / Nutanix</i>
<ul style="list-style-type: none"> <li>• <i>Listado completo de equipos y modelos, diagrama físico, velocidad y tipo de conexiones físicas, detalles del contenido y espacio en U (unidades de rack) para el rack. Además, para los software y licencias se deberá presentar modelos, detalles de funcionalidad incluidas y versiones</i></li> </ul>

## Criterios de desempate de ofertas

En caso de que existan dos o más oferentes solventes que cumplan con todos los requisitos establecidos en el pliego de bases y condiciones del llamado, igualen en precio y sean sus ofertas las más bajas, el comité de evaluación determinará cuál de ellas es la mejor calificada para ejecutar el contrato utilizando los criterios dispuestos para el efecto por la DNCP en la reglamentación pertinente.

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





# SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS

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

## Suministros y Especificaciones técnicas

El Suministro deberá incluir todos aquellos ítems que no hubiesen sido expresamente indicados en la presente sección, pero que pueda inferirse razonablemente que son necesarios para satisfacer el requisito de suministro indicado, por lo tanto, dichos bienes 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 registrará de conformidad a la cláusula de adendas y cambios.

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

## Detalle de los productos con las respectivas especificaciones técnicas

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

### Antecedentes

En carácter de entidad reguladora, controladora y certificadora de la calidad, eficacia y seguridad de medicamentos, tecnología, materiales y todo producto de uso y aplicación en medicina humana y productos considerados cosméticos, Domi sanitarios y tabaco.

Surge la imprescindible necesidad de actualización tecnológica para responder a la demanda, siendo esta situación acentuada por la pandemia del COVID-19.

La DNVS requiere la provisión, instalación, configuración y puesta en producción de una arquitectura de misión crítica, robusta, confiable, escalable, flexible, segura y resiliente. Para ello la DNVS deberá actualizar su infraestructura tecnológica de manera a soportar la nueva demanda de servicios.

El proyecto global constara de 5 pilares principales, que serán ejecutados en distintas etapas:

- Reingeniería de la Infraestructura de Cómputo. Presente llamado.
- Implementación de un nuevo sistema de gestión.
- Virtualización de escritorios.
- Readecuación de la red física.
- Digitalización de documentos.

Para cumplir con los pilares definidos, la infraestructura a ser adquirida debe componerse de un equipamiento de red robusto, servidores de alto rendimiento y también, una solución de backup bien preparada ante posibles contingencias. Toda la plataforma debe ser escalable y segura, que soporte ambientes altamente virtualizados y una amplia variedad de cargas de trabajo, que funcione como una única solución. Todas las soluciones ofertadas deben ser totalmente compatibles con los servicios, configuraciones y aplicaciones existentes.

## Objetivos Específicos

La solución a ser adquirida deberá permitir cumplir con los siguientes objetivos específicos:

- **Confiabilidad:** la solución debe proponer no solo hardware y software confiables, sino que debe ser líder en el mercado, demostrando de esta manera que la solución propuesta está respaldada por una gran cantidad de casos de éxito en diferentes ámbitos.
- **Escalabilidad:** se deben proveer funciones de escalamiento lineal. Debe soportar la ampliación de nodos de manera granular, en diferentes modelos y tamaños, que se adapten a las necesidades actuales y que ya no sea necesario aprovisionar la infraestructura por adelantado.
- **Resiliencia:** la solución debe tener capacidad de adaptación y recuperación ante fallas que puedan surgir y seguir operando en las mejores condiciones posibles.
- **Seguridad:** la solución debe contar con un diseño de seguridad asumiendo que cualquier red, aplicación, servidor o usuario podría verse comprometido. Basándose en esta suposición, todos los protocolos de seguridad deben apuntar a esto, desde el ciclo de vida de desarrollo del software, automatización de procesos de mantenimiento, políticas perimetrales de seguridad de la red, gestión de identidad y acceso, cifrado de datos, cumplimiento de normativas, auditoría y reportes.
- **Tolerante a fallos:** las soluciones deben funcionar con tolerancia a fallos a nivel de servidores y switches, limitando al mínimo el riesgo de interrupciones en los servicios ante la falla de uno de estos componentes.

### Marco General

El proyecto de Reingeniería de la infraestructura de cómputo ha sido desarrollado por el área de tecnología de la DNVS en el que se comprende; 1 (un) Datacenter ubicados en edificio de la DNVS, así como toda la infraestructura de seguridad, cómputo, almacenamiento y comunicaciones que brindan el soporte actualmente a las aplicaciones de la DNVS.

A tal efecto fueron elaboradas las especificaciones técnicas para la adquisición de una infraestructura tolerante a fallos, que comprende: Solución Hiperconvergente, Equipos de Comunicaciones, Equipos de Seguridad Avanzados, Hardware y Software de Backup, Antivirus, Licenciamiento Microsoft y Racks Autónomos.

Los Proveedores deberán ser capaces de suministrar, instalar, configurar, mantener y dar soporte a toda la solución ofrecida y que permita satisfacer los requerimientos de la DNVS detallados en este documento para cada ítem. Debiendo proporcionar total compatibilidad teniendo en consideración los requerimientos establecidos en la Sección III del PBC.

La solución deberá utilizar una plataforma hiperconvergente, mediante equipos que posean características y funcionalidades de escalamiento y crecimiento modular conforme los requerimientos que sean demandados en el futuro. Esta plataforma hiperconvergente debe ser 100% compatible con la solución hiperconvergente donada a la DNVS para una administración centralizada de toda la solución.

Así mismo, se requiere una solución para virtualización de escritorios y aplicaciones. Esta solución deberá ser 100% compatible e integrable al Software de virtualización de escritorios y aplicaciones de la DNVS.

Es requisito imprescindible que se garantice y asegure la interoperabilidad y funcionamiento de toda la solución, incluido todo el equipamiento necesario. A fin de salvaguardar este requerimiento, el Oferente deberá proveer equipos y/o sistemas que sean compatibles con las especificaciones técnicas de los demás lotes o ítems a fin de garantizar el perfecto funcionamiento de todos los elementos componentes.

El conjunto deberá tener herramientas con capacidad de visualización centralizada para monitoreo, además capacidad de gestión completa, ágil y sencilla para la infraestructura de cómputo, redes y almacenamiento en entornos físicos y virtuales.

La contratación incluye:

- Provisión, instalación, configuración y soporte de todo el hardware y software solicitados en este llamado.
- Provisión y cableado (eléctrico y de datos) de los equipos solicitados.
- Profesionales capacitados necesarios a fin de que todo el sistema sea entregado bajo un preciso ajuste de funcionamiento, conforme a los requerimientos de instalación de los fabricantes de los equipos.
- Provisión de materiales, accesorios y servicios necesarios para la puesta en marcha de todos los equipos, nodos y software certificados solicitados.
- Acompañamiento y transferencia de conocimiento al personal operativo de la DNVS.
- Las demás prestaciones establecidas en el presente PBC (Soporte, actualizaciones, garantías, etc.).
- Integración de todos los productos, nodos y software entregados con los equipos y/o sistemas correspondientes a los demás ítems, de tal forma a que éstos queden listos para ser utilizados.

La presente descripción es meramente enunciativa y no es limitante a cualquier otra tarea que sea requerida para la correcta ejecución e implementación de todo lo requerido.

### Sistemas Requeridos

Comprende la provisión, instalación incluyendo todos los accesorios y materiales necesarios, puesta en funcionamiento y configuración de los servicios de hardware y software de un conjunto de equipos informáticos compuesto por los siguientes:

ITEM	DESCRIPCIÓN	CANTIDAD
1	RACKS INTELIGENTES	2 (dos)
2	SISTEMA DE COMPUTO HIPERCONVERGENTE PARA VIRTUALIZACIÓN DE SERVIDORES	1 (uno)
3	EQUIPOS DE SEGURIDAD (NEXT GENERATION FIREWALL)	1 (uno)
4	EQUIPOS DE RED (SWITCHES ToR)	2 (dos)

ESPECIFICACIONES TÉCNICAS DE LAS SOLUCIONES REQUERIDAS:		
ITEM 1 RACK INTELIGENTE		
Características	Especificaciones	Requerimiento
Marca	Especificar	Exigido
Modelo	Especificar	Exigido
Cantidad	2 (dos)	Exigido

GENERAL	<p>Sistema deberá estar formado por un rack cerrado integrado, dotado de soporte ambiental, energía y monitoreo preensamblado de fábrica, contando con un único número de parte y número de serie.</p> <p>Las características generales que deberá cumplir son las siguientes:</p> <ul style="list-style-type: none"> <li>- Dimensiones externas del gabinete (ancho x profundidad x alto): 600 × 1200 × 2000 mm</li> <li>- Puerta delantera y trasera vidriada</li> <li>- Altura interna disponible para montaje de equipos: 29U (1U = 44.45mm)</li> <li>- Profundidad disponible para montaje de equipos: 721.5 mm</li> <li>- Potencia disponible para equipos de TI <math>\leq</math> 3kW (Máxima permitida 3kW)</li> <li>- Tensión (Vca) monofásica: 220Vca / rango admisible:198-254 Vca</li> <li>- Frecuencia: 50/60 Hz</li> <li>- Modo de enfriamiento: integrado con contención fría y caliente</li> <li>- Grado de protección: IP5X</li> <li>- Peso: &lt; 300kg</li> <li>- Capacidad máxima de carga del rack: 1300 Kg</li> <li>- Nivel de ruido: la unidad interior no excederá los 50 dB. La unidad interior con condensador no excederá los 58dB</li> <li>- PUE general del sistema: no deberá exceder 1.60</li> <li>- Certificaciones: ISO 9001; IEC60950-1; EMC Tests de acuerdo a EN55022:2010, EN 55024:2010, EN61000-3-11:2000, EN61000-3-12:2011; IP5x Tested; ISO14001:2004, ISO9001:2008, OSHAS18001:2007.</li> </ul> <p>Todos los componentes del Rack deberán ser del mismo fabricante.</p> <p>La Empresa oferente deberá montar los equipos en las instalaciones indicadas por la Institución y deberá proveer todos los componentes eléctricos para su instalación.</p> <p>La empresa oferente deberá trasladar los servidores y todo lo necesario al nuevo rack dejando el mismo funcionando en un periodo de tiempo no mayor a 24 hs. La migración se realizará en los días establecidos por la institución.</p>	Exigido
---------	--	---------

<b>CARACTERÍSTICAS ESTÁNDAR</b>	<p>El sistema deberá disponer de protección ante la presencia de polvo, aislación para reducción del nivel de ruido audible, alta eficiencia y ahorro de energía, enfriamiento con circuito cerrado con control de temperatura, humedad y pureza del aire para prolongar la vida del equipamiento de TI. Contendrá internamente una UPS de alta eficiencia diseñada para el uso en centros de datos y un aire acondicionado de precisión con tecnología de contención fría y caliente, para mejorar la eficiencia de enfriamiento. El ventilador interno será de bajo nivel de ruido, apto para su aplicación dentro de oficinas.</p> <p>Monitoreo inteligente: deberá contar con funciones de control inteligentes, tales como el monitoreo del ambiente integrado, monitoreo de equipos, manejo de alarmas y demás funciones, para proporcionar una plataforma de monitoreo centralizada desde el centro de datos.</p> <p>Ahorro de energía e integración total: el gabinete deberá proveer las condiciones de operación estables para todos los equipos de TI en su interior. Se requerirá únicamente la conexión al gabinete y al aire acondicionado en el sitio de montaje. El sistema ocupará como máximo una superficie de 0.75 m2.</p> <p>Debe contar con sistema que cuente de una pantalla LCD de 9 del tipo táctil en su puerta frontal para informar la condición de operación, alarmas e información de seguridad.</p> <p>Debe contar con una placa de monitoreo, se podrá realizar el monitoreo remoto del sistema durante las 24 hrs.</p>	Exigido
<b>ADMINISTRACION</b>	<p>Debe incluir un Conmutador Switch KVM de 8 puertos o superior.</p> <p>Consola KVM Digital 8 puertos o superior, 1U, pantalla LCD 17 como mínimo.</p> <p>Paquetes de Módulos USB VM LCD (KVM-USBVM).</p> <p>Kit de Soporte KVM/LCD.</p> <p>Compatibles con Windows y Linux</p> <p>Led de Estado</p> <p>Software incluido perpetuo, ambiente web.</p> <p>Cables y adaptadores de acuerdo con la cantidad de puertos.</p>	Exigido
<b>SISTEMA DE RACKS</b>	<p>El sistema deberá contar internamente con guías 19 para el montaje del equipo de TI que cumplirán con la norma EIA-310-D.</p> <p>El gabinete estará herméticamente cerrado mientras funcione, para mantener los equipos libres de polvo, y acondicionados, ahorrando energía y reduciendo el nivel de ruido.</p> <p>Las puertas vidriadas frontal y trasera actúan como contención fría y caliente respectivamente.</p>	Exigido
<b>ALIMENTACION Y DISTRIBUCION</b>	<p><b>Debe incluir los siguientes componentes</b></p> <ul style="list-style-type: none"> <li>- PMU (Unidad de Manejo de Energía): esta unidad brindará la distribución de energía y la protección contra sobretensiones transitorias al todo el sistema. Dispondrá de una entrada de red y múltiples salidas a cada una de las cargas internas.</li> <li>- UPS y banco de baterías: esta unidad proveerá energía de alta calidad y de alta disponibilidad para las cargas de TI.</li> <li>- Sistema(s) de Distribución de Energía (PDU): estará dotado de la capacidad de apagar o encender inteligentemente los tomacorrientes de salida y medir los parámetros eléctricos de entrada y salida</li> <li>- Iluminación auxiliar interna de LED</li> </ul>	Exigido

### **Unidad de Administración de Energía (PMU)**

El PMU es un tablero de interruptores que debe proveer la distribución de energía y la protección contra sobretensiones transitorias (Clase C) y es la única entrada de energía al sistema

Incluye las siguientes entradas y salidas:

Al menos una entrada de alimentación principal

Al menos un Bypass de mantenimiento para UPS

Al menos una entrada de UPS y una salida de UPS

Al menos una salida a la unidad de refrigeración

Al menos una salida de 16A para PDU

Al menos dos salidas de 16A para reserva.

Al menos una salida CC

### **Unidades de distribución de energía (PDU)**

Al menos una PDU de 24 tomacorrientes, compuesto de: 18 x C13 + 6 x C19; El rack debe tener capacidad de instalar al menos un total de 2 PDU

### **UPS y sistema de batería**

La UPS deberá ser de montaje en rack con una potencia de 6kVA/4.8kW para soportar las cargas de TI y el sistema de ventilación de emergencia.

Las especificaciones mínimas del UPS serán como sigue:

- Rectificador del tipo IGBT
- Del tipo On-line doble conversión
- Factor de potencia de entrada >0.99
- Rango de frecuencia de entrada: 40Hz to 70Hz
- Rango de tensión de entrada a plena carga: 185Vca to 280Vca
- Tensión de salida monofásica 220Vca
- Tensión de entrada monofásica 220Vca, L-N + T
- La UPS cumplirá con: IEC/EN62040-1-1; EMC IEC / EN 62040-2, IEC / EN61000-3-11, IEC / EN61000-3-12, YD / T1095-2008; Surge Protection IEC / EN 61000-4-5; Protection Level IP20
- Banco de batería interno, del tipo sellada, electrolito absorbido, libre de mantenimiento, de plomo-ácido, tipo VRLA
- Capacidad de carga de la batería: al menos 3 horas hasta el 90% de su capacidad.
- Dimensiones del UPS con baterías: 430 x 574 x 217 mm y peso: 60 kg
- La autonomía será de un mínimo de 10 minutos a carga típica (75% de carga)
- Eficiencia mínima CA-CA: 92%en rack: batería de plomo-ácido sellada, sin derrames, sin mantenimiento

Se debe prever lo siguiente para la instalación y puesta en marcha:

Instalación de un tablero con llaves independientes, conectado al generador eléctrico con sistema de tierra.

Proveer de cableado para la sala de informática con puntos de tomacorriente con un sistema de tierra y canaletado, conectado al tablero al ser instalado.

Para el suministro de energía de la llave principal la misma deberá estar conectada en forma independiente al tablero, el cableado suministrado deberá venir del tablero central que también deberá contar con una llave.

Los materiales para las instalaciones, conexión y puesta en funcionamiento deberán estar a cargo del oferente.

Las Tomas Corrientes deberán ser la cantidad necesaria, Dirección Informática

	<p>y Mesa de Entrada.</p> <p>Las luces, fluorescentes, aires acondicionados deberán estar cargados al nuevo tablero.</p> <p>Instalación de un tablero de pared adecuado para el proyecto con cerradura.</p> <p>Remoción del cableado, canaletado, toma corriente y disyuntores viejos.</p>	
<b>SISTEMA DE REFRIGERACIÓN</b>	<p><b>Deberá incluir los siguientes componentes:</b></p> <p>Aire acondicionado: su función es enfriar activamente los dispositivos electrónicos dentro del gabinete, para lo cual se proveerá un pequeño equipo de acondicionamiento ambiental de precisión, del tipo inverter (tecnología de conversión de frecuencia), especialmente diseñado para el enfriamiento de dispositivos electrónicos, con alta eficiencia energética y regulación automática, manteniendo el ambiente estable dentro del gabinete, permitiendo que los equipos de TI operen con seguridad y confiabilidad</p> <p><b>Aire acondicionado</b></p> <p>Dispondrá de 2 partes:</p> <ul style="list-style-type: none"> <li>- Unidad evaporadora interior, con ventilador incorporado dentro del rack</li> <li>- Unidad condensadora exterior con compresor del tipo inverter (tecnología de conversión de frecuencia) utilizando refrigerante ecológico R410a</li> <li>- Capacidad de enfriamiento disponible: 3 kW</li> <li>- Eficiencia energética: consumo máximo de entrada 1.5kW</li> <li>- Rango de frecuencia: 50Hz±3Hz</li> <li>- Corriente máxima de operación: 7A</li> </ul> <p><b>Sistema de ventilación de emergencia</b></p> <p>Este sistema evitará las sobreelevaciones de temperatura dentro del gabinete en caso de ocurrir una falla en el sistema de enfriamiento.</p> <p>En el caso que ocurra una sobretemperatura, detención o falla del equipo de aire acondicionado, este sistema de emergencia arrancará automáticamente para prevenir que el equipo de TI funcione a alta temperatura. Cuando el sistema se halla operando normalmente, la ventilación de emergencia estará apagada, para asegurar la hermeticidad del sistema y la alta eficiencia del aire acondicionado.</p> <p>Cada módulo de ventilación contendrá 3 ventiladores.</p>	Exigido

<b>VIGILANCIA</b>	<p><b>Todos los componentes del sistema deberán ser instalados en fábrica dentro del gabinete integrado.</b></p> <p>1 x Placa de monitoreo</p> <p>2 x Sensores inteligentes de temperatura (1 para montaje frente, 1 para montaje posterior)</p> <p>1 x Detector de agua del tipo cinta</p> <p>2 x Entradas para sensores inteligentes con puertos RJ45</p> <p>La placa de monitoreo Web/SNMP, podrá monitorear el estado de los dispositivos inteligentes del sistema, grabar eventos de alarma y notificar al usuario de dichas alarmas a través de correo electrónico o mensajes SMS. Esta placa también posibilitará el seteo de parámetros de operación y visualizar el estado de los dispositivos a través del HMI Web embebido, además, podrá enviar los estados de los dispositivos inteligentes monitoreados al Software de Administración de Red (NMS) a través de protocolo SNMP</p> <p>El paquete de monitoreo estándar incluirá las siguientes características:</p> <ul style="list-style-type: none"> <li>- Manejo de alarmas</li> <li>- Historial de alarmas</li> <li>- Administración de equipos</li> </ul>	Exigido
<b>CONDICIONES ESPECIFICAS</b>	<p>Que la Empresa oferente debe contar con el soporte de la empresa certificadora de la marca en el país.</p> <p>Presentar con la oferta autorización del fabricante expresamente dirigido a la entidad mencionando la licitación específica</p> <p>La instalación podrá ser realizada por el proveedor del rack inteligente o por la marca del rack a través de sus representantes y/o canales que operen dentro del país. La correcta instalación deberá quedar certificada por escrito.</p>	Exigido
<b>Instalación</b>	El proveedor deberá montar y configurar apropiadamente el rack en las instalaciones de la DNVS, para lo cual proveerá todos los accesorios e insumos para la instalación y configuración de toda la solución.	Exigido
<b>Garantía (Escrita)</b>	<p>Cartas del fabricante y/o representante oficial donde se especifique una garantía de al menos 3 Años para soporte de atención sobre el Hardware, así como también la provisión de repuestos del hardware durante el mismo periodo mencionado.</p> <p>El soporte de atención debe ser 7x24 con 4 horas de tiempo de respuesta por parte del soporte local para la primera atención, tanto para el hardware como para el software.</p>	Exigido
<b>Certificaciones requeridas</b>	Certificado de calidad mínimamente ISO9001 del fabricante.	Exigido
<b>Compatibilidad</b>	Todos los componentes de cada solución integrada deben estar certificados para funcionar correctamente entre sí.	Exigido

## ÍTEM 2: SISTEMA DE COMPUTO HIPERCONVERGENTE PARA VIRTUALIZACIÓN DE SERVIDORES



Características	Especificaciones	Requerimiento
Cantidad	1 (uno)	Exigido
Marca	Especificar	Exigido
Modelo	Especificar	Exigido
Factor de Forma	Chasis Rackeable	Exigido
Tamaño Máximo de la Solución	4U	Exigido
Plataforma	La solución de hiperconvergencia requerida deberá ser implementado e integrado al clúster de cómputo hiperconvergente Nutanix existente de la DNVS. Para cumplir con este requerimiento, se debe garantizar total compatibilidad, integración e interoperabilidad entre los mismos.	Exigido
Arquitectura de procesadores	Intel x86 64 bits.	Exigido
Capacidad de procesamiento	Mínimo 72 núcleos de 2.4 GHz con memoria caché de 16 MB o superior en la solución ofertada. Escalable de manera ilimitada .	Exigido
Capacidad de Memoria	Mínimo de 768GB DDR4 3200 MHz en la solución ofertada. Escalable de manera ilimitada .	Exigido
Capacidad de Almacenamiento	Mínimo de 46TB RAW en discos de estado sólido (SSD) y 240TB RAW en discos de capacidad (HDD) en la solución ofertada. Escalable de manera ilimitada.	Exigido
Administración	<p>El marco de administración debe proporcionar una interfaz de usuario gráfica intuitiva. Toda la información se debe organizar y presentar a través de áreas bien definidas con el propósito de lograr un acceso sencillo a los datos operativos. Debe ofrecer la capacidad de definir y administrar una infraestructura convergente completa desde cualquier dispositivo.</p> <p>Deberá ser integrada a la solución de cómputo hiperconvergente existente en la DNVS y proveer una herramienta que permita tener visibilidad de todos los servidores/nodos/hosts y sus recursos desde una consola de administración única.</p>	Exigido
Conexión LAN	Módulos de interconexión Ethernet con 2 puertos 10GbE con módulos SFP+ por cada servidor/nodo/host.	Exigido

	<p>Se deberá contar con módulos de interconexión LAN internos al chasis, cada servidor/nodo/host con 2 puertos externos activados (SFP+) de corta o larga distancia de 10Gbps o superior.</p>	
	<p>La solución debe poder funcionar con switches Ethernet 10GbE de varias marcas.</p>	
	<p>Todos los cables necesarios para la conexión LAN deberán ser proveídos.</p>	
<b>Ventiladores y fuentes de alimentación</b>	<p>El sistema de ventilación (coolers) y el sistema de alimentación provisto, deberán estar preparados para soportar la instalación completa del chasis con sus bahías completas, sin producir una degradación general del sistema. Las fuentes de alimentación deberán ser redundantes.</p>	Exigido
<b>Alimentación Eléctrica</b>	<p>La alimentación Eléctrica de los servidores/nodos/hosts deberá ser de tipo Redundante (1+1).</p> <p>Alimentación: 220 voltios corriente alterna monofásico.</p>	Exigido
	<p>Frecuencia en Hertz 50/60</p>	Exigido
<b>Herramienta / Consola de gestión o Administración</b>	<ul style="list-style-type: none"> <li>La interfaz de administración deber ser accedida mediante un browser y estar basada en HTML5.</li> </ul>	Exigido
	<ul style="list-style-type: none"> <li>Proveer una única vista para todo el entorno manteniendo múltiples puntos de acceso.</li> </ul>	
	<ul style="list-style-type: none"> <li>La consola de Administración deberá ejecutarse sobre los mismos servidores/nodos/hosts del Clúster que administra, aprovechando la tolerancia a fallos del mismo (Ej. La consola debe permanecer disponible ante la falla de cualquiera de los servidores/nodos/hosts).</li> </ul>	
	<ul style="list-style-type: none"> <li>Proveer accesos alternativos basados en SSH y/o interfaces remotas estilo IPMI.</li> </ul>	
	<ul style="list-style-type: none"> <li>Contener autenticación LDAP, Active Directory, CAC Authentication y certificados firmados por SSL.</li> </ul>	
	<ul style="list-style-type: none"> <li>Contemplar integración mediante el uso de REST API a otras soluciones de administración, a fin de facilitar la integración con ambientes de monitoreo actuales.</li> </ul>	

	<ul style="list-style-type: none"> <li>• Tener la capacidad de facilitar una consola gráfica, que permita visualizar los recursos utilizados por las máquinas virtuales (VM) independientemente del tipo de hipervisor.</li> </ul>	
<b>Almacenamiento</b>	La solución debe contar con un sistema de almacenamiento distribuido definida por software y proveer las siguientes funcionalidades:	Exigido
	<ul style="list-style-type: none"> <li>• Cada servidor/nodo/host, deberá contar con su propia controladora de almacenamiento.</li> </ul>	
	<ul style="list-style-type: none"> <li>• Esquema de capas en forma automática (tiering) entre los diferentes niveles, memoria, disco de estado sólido (SSD), y discos mecánicos (HDD) en tiempo real.</li> </ul>	
	<ul style="list-style-type: none"> <li>• Deduplicación de tres niveles, en la ingesta de información, en los discos de estado sólido (SSD) y en los discos mecánicos (HDD).</li> </ul>	
	<ul style="list-style-type: none"> <li>• Compresión tanto en línea y en reposo.</li> </ul>	
	<ul style="list-style-type: none"> <li>• Snapshots basados en punteros.</li> </ul>	
	<ul style="list-style-type: none"> <li>• Sistemas de clones de máquinas virtuales.</li> </ul>	
	<ul style="list-style-type: none"> <li>• Capacidad de usar Erasure Coding para poder hacer uso eficiente del espacio en discos mecánicos (HDD)</li> </ul>	
	<ul style="list-style-type: none"> <li>• Debe existir un sistema que permita que a lo largo del tiempo los datos más accedidos por una VM corriendo en cualquiera de los servidores/nodos/hosts, tengan siempre una copia en el almacenamiento del servidor/nodo/host local, de manera que la lectura pueda realizarse a velocidad local en la mayoría de los accesos. Este mecanismo debe converger y actualizarse de manera automática si la VM es movida/trasladada a otro servidor/nodo/host.</li> </ul>	
	<ul style="list-style-type: none"> <li>• Thin Provisioning tanto para máquinas virtuales, como a nivel de contenedor/datastore.</li> </ul>	
	<ul style="list-style-type: none"> <li>• Capacidad de réplica en forma sincrónica o asincrónica.</li> </ul>	
	<ul style="list-style-type: none"> <li>• La réplica de los datos debe poder configurarse con granularidad por Máquina Virtual (VM)</li> </ul>	

	<ul style="list-style-type: none"> <li>El clúster debe poder replicar contra otro/s Clúster/s de similares características en el sitio local o en sitios remotos de manera sencilla. Adicionalmente, la solución de réplica debe de permitir replicar máquinas virtuales entre hipervisores diferentes para poder facilitar la migración de un hipervisor a otro.</li> </ul>	
	<ul style="list-style-type: none"> <li>El almacenamiento debe estar diseñado especialmente para ambientes virtualizados.</li> <li>La solución de Software-Defined Storage (SDS) ofrecida deberá ser agnóstica al Hipervisor. Debe permitir al usuario cambiar el Hipervisor de base y así soportar distintos hipervisores a elección del cliente. Debe ser compatible mínimamente con VMware ESXi, Microsoft Hyper-V e hipervisores basados en Linux/KVM.</li> </ul>	
	<ul style="list-style-type: none"> <li>La arquitectura de almacenamiento debe permitir que cada servidor/nodo/host vaya integrado con una controladora para gestionar los recursos de almacenamiento en un clúster, y para todas las máquinas virtuales. Estas controladoras deben comunicarse entre sí, permitiendo gestionar el acceso desde múltiples servidores/nodos/hosts a los datos replicados.</li> <li>La solución debe tener la capacidad de generar un volumen de almacenamiento tipo bloque que pueda ser presentado a servidores externos (físicos o virtuales) mediante el protocolo iSCSI.</li> </ul>	
	<ul style="list-style-type: none"> <li>La solución de almacenamiento no debe requerir de switches de Fibre Channel ni FCoE para su funcionamiento. Solamente utilizará IP sobre Ethernet estándar. No deberá ser obligatorio configurar características específicas como Jumbo-Frames, ni otras características especiales para lograr que el Clúster opere correctamente.</li> </ul>	
	<ul style="list-style-type: none"> <li>Deberá tener la capacidad de distribuir los datos adentro del clúster y adicionalmente poder replicarlos internamente, para poder asegurar su disponibilidad. El factor de réplica puede ser configurado en modo 2 ó 3, dependiendo de la cantidad de nodos instalados.</li> <li>La solución deberá tener la capacidad de realizar respaldos a AWS (Amazon Web Services) y Microsoft Azure.</li> </ul>	
Escalabilidad	<ul style="list-style-type: none"> <li>Proveer un crecimiento lineal, estable y predecible en su rendimiento a medida que se agreguen servidores/nodos/hosts. Soportar un crecimiento ilimitado en servidores/nodos/hosts, que incrementen la capacidad de procesamiento, memoria y almacenamiento. El clúster una vez establecido debe ser capaz de crecer de a un servidor/nodo/host por vez.</li> </ul>	Exigido
	<ul style="list-style-type: none"> <li>Deberá soportar crecimiento lineal con servidores/nodos/hosts heterogéneos, o de diferentes modelos para maximizar recursos de procesamiento, memoria o almacenamiento según se requiera.</li> </ul>	
	<ul style="list-style-type: none"> <li>Proveer la factibilidad de crecimientos modulares evitando así el sobre-dimensionamiento del proyecto.</li> </ul>	

	<ul style="list-style-type: none"> <li>• El crecimiento tiene que ser en forma granular de hasta un servidor/nodo/host por vez incrementando los recursos globales de procesamiento, memoria, y almacenamiento en forma simultánea de todo el cluster y en diferentes proporciones, para poder acomodarse a los diferentes requerimientos.</li> </ul>	
<b>Tipos de nodos</b>	Se debe poder integrar servidores/nodos/hosts con diferentes características que le permitan adaptarse a los requerimientos de cada una de las aplicaciones y formando un clúster mixto.	Exigido
	Los tipos de nodos esperados son:	
	<ul style="list-style-type: none"> <li>• Intensivos en Computo (CPU/Memoria).</li> </ul>	
	<ul style="list-style-type: none"> <li>• Intensivos en Almacenamiento.</li> </ul>	
	<ul style="list-style-type: none"> <li>• Nodos solamente con discos SSD.</li> </ul>	
<b>Alta Disponibilidad</b>	La infraestructura de Cómputo y Almacenamiento deberá ser distribuida y completamente definida por software, armando un clúster con las siguientes características:	Exigido
	<ul style="list-style-type: none"> <li>• Filesystem con capacidad de recuperación ante la falla de un disco o de un servidor/nodo/host completo que forma parte de la solución.</li> </ul>	
	<ul style="list-style-type: none"> <li>• La protección de los datos deberá ser realizando múltiples copias de los datos en los discos pertenecientes a más de un servidor/nodo/host, de manera a garantizar que los datos sigan disponibles aún luego de la falla de algún componente o incluso la falla de un servidor/nodo/host completo (tolerancia a fallos).</li> </ul>	
	<ul style="list-style-type: none"> <li>◦ Esta protección de datos deberá realizarse entre los múltiples servidores/nodos/hosts que componen el Clúster, de manera distribuida</li> </ul>	
	<ul style="list-style-type: none"> <li>◦ En caso de una falla, la solución basada en Software debe actuar de manera automática creando nuevas copias múltiples de los datos, de manera a mantener el nivel de protección hasta tanto se reemplace el componente que haya fallado (Auto-Saneamiento de la solución)</li> </ul>	
<b>Licencias</b>	<p>Se deberá incluir en la oferta las siguientes licencias de Sistema Operativo:</p> <ul style="list-style-type: none"> <li>◦ 6 (seis) licencias de Sistemas Operativos Server Estándar</li> <li>◦ 100 (cien) Licencias de acceso de usuarios a Servidor, CAL de acceso.</li> </ul>	Exigido

<b>Instalación</b>	<b>Alcance:</b> El servicio contemplará todos los suministros, actividades de montaje, instalación en general, configuración y puesta en funcionamiento de la solución ofertada en el gabinete designado por el DNVS. La instalación deberá ser realizada con la presencia de técnicos del DNVS.	Exigido
	<b>Accesorios:</b> Los accesorios de montaje en el Rack serán proveídos por el oferente y deberá incluir todo el kit con cables, soportes, organizadores y demás accesorios requeridos. El proveedor deberá montar y configurar apropiadamente en el rack para alojar la solución, para lo cual proveerá todos los accesorios e insumos para la instalación. Se deben proveer los cables necesarios para establecer la conectividad entre los equipos hiperconvergentes y el switch ofertado con la solución.	Exigido
<b>Garantía (Escrita)</b>	Soporte de atención de Hardware y Software, Mano de Obra y Repuestos (cualquier daño de componentes de los equipos deberá ser cambiado o reparado) incluyendo traslado de los equipos de la oficina del cliente al proveedor y viceversa a cargo del proveedor. Si la reparación implica la indisponibilidad del equipo por 24 hs. o más, el proveedor suministrará otro equipo mientras dure la reparación del mismo. El soporte de atención debe ser 7x24, la Mano de Obra y Repuestos locales deben estar incluidos.	3 años
<b>Soporte de Mantenimiento Preventivo</b>	Soporte de mantenimiento preventivo del equipo proveído, mano de obra incluyendo limpieza de componentes, durante la vigencia de la garantía, a cargo del proveedor. Se requieren un mínimo de 20 (veinte) horas anuales para esta finalidad.	
		3 años
<b>Capacitación</b>	El Oferente Adjudicado deberá proveer todos los recursos para el entrenamiento teórico y práctico a los técnicos de la DNVS en la instalación, configuración y administración de los equipos ofertados, tales como:	Exigido
	<ul style="list-style-type: none"> <li>• Instalación de los sistemas operativos de los equipos y las configuraciones necesarias para brindar diferentes servicios y ampliaciones.</li> </ul>	
	<ul style="list-style-type: none"> <li>• Operar los equipos realizando tareas de monitoreo, pruebas y ajustes en servicios necesarios para mantener el sistema en condiciones de operación normal.</li> </ul>	
	<ul style="list-style-type: none"> <li>• Mantener el equipamiento en su estado operacional nominal a través de un programa de mantenimiento preventivo y correctivo.</li> </ul>	
	<ul style="list-style-type: none"> <li>• Instrucciones y procedimientos para mantenimientos de emergencia.</li> </ul>	
	Se deberá ofrecer una capacitación con certificados, destinada a 2 (dos) funcionarios técnicos de DNVS, con una duración mínima de 10 horas.	

	La capacitación deberá ser realizada en las instalaciones DNVS. Esta capacitación deberá ser realizada en un plazo máximo de 8 meses, para lo cual el Oferente deberá de presentar una Carta Compromiso a través de la cual se compromete a realizar dicha capacitación.	
<b>Consideraciones Generales</b>		
	<ul style="list-style-type: none"> <li>El Oferente deberá presentar Garantía de los Bienes y Servicios ofertados por el término de 3 (tres) años. Dentro de este periodo, el Oferente repondrá gratuitamente dentro de los límites de la República del Paraguay, en cualquier lugar o donde ocurriere la falla, cualquier pieza o conjunto de piezas que fallaren, se rompan, se desgasten prematuramente, debido al diseño, material o fabricación defectuosa o mal montaje por parte del Oferente. Esta garantía empezará desde el día de la puesta en marcha de los equipos en producción. La garantía deberá estar disponible 24x7x365, con 4 horas de tiempo de respuesta, tanto para el hardware, software, así como toda la solución ofertada, con disponibilidad inmediata de repuestos y equipos.</li> </ul>	Exigido
	<ul style="list-style-type: none"> <li>De surgir algún inconveniente en la instalación de los bienes originada por una incorrecta especificación, el Contratante no aceptará reclamos o justificará fallas en los programas, por lo que de producirse una de estas situaciones resultarán de automática aplicación las penalidades que, por atrasos, fallas, etc. se establezcan en el Contrato.</li> </ul>	
	<ul style="list-style-type: none"> <li>Los equipos deben ser nuevos y de última generación para la familia de equipos ofertados. Los equipos no deben tener fecha de finalización de comercialización publicada.</li> </ul>	
	<ul style="list-style-type: none"> <li>La falta de algún elemento (hardware, software y/o cualquier componente o partes) necesario para el funcionamiento de los bienes, tanto individualmente, cuanto en operación conjunta, para los fines funcionales previstos por el Contratante, originado por cualquier tipo de interpretación de las especificaciones técnicas, obligará al oferente a proveerlo de inmediato y sin cargo adicional para el Contratante. Las adecuaciones que fueran necesarias realizar para dar cumplimiento a lo establecido precedentemente serán realizadas por el Contratante en coordinación con el Oferente y garantizando en todos los casos la preservación de la funcionalidad requerida.</li> </ul>	
	<ul style="list-style-type: none"> <li>Todos los equipos a proveer deberán ser nuevos, sin uso y en perfecto estado de funcionamiento. Todo bien a suministrar deberá pertenecer a la línea actual de productos del fabricante, y ser el más reciente estable en dicha línea.</li> </ul>	
	<ul style="list-style-type: none"> <li>La entrega de cualquier Software significará la entrega de las Licencias de Uso del Software, emitidas a nombre del Contratante como mínimo durante el periodo que dure la garantía.</li> </ul>	

	<ul style="list-style-type: none"> <li>El Oferente entregará, conjuntamente con los bienes contratados, toda bibliografía técnica considerada necesaria para su utilización, actualizada a la última versión y con la obligación permanente, durante la vigencia de la garantía de buen funcionamiento, de remitir toda modificación. La documentación deberá estar escrita en idioma castellano u opcionalmente en inglés, cuando no existiese versión en aquel idioma. En todos los casos deberá proveer al menos una copia material de la documentación (impreso o en CD-ROM/DVD).</li> </ul>	
	<ul style="list-style-type: none"> <li>El Oferente deberá proveer toda la documentación de los bienes ofertados, se entiende por estas documentaciones al conjunto de literaturas técnicas para la instalación, operación, funcionamiento, detección y prevención de fallas, condiciones de uso de los equipos; e instalación, explotación, operación y solución de fallas del software.</li> </ul>	
	<ul style="list-style-type: none"> <li>No se tendrán en cuenta las ofertas que no presenten toda la información solicitada en las Consideraciones Generales, ya que ello no ofrecería la suficiente garantía para el buen funcionamiento de los equipos.</li> </ul>	

ITEM 3 EQUIPOS DE SEGURIDAD (NEXT GENERATION FIREWALL)		
Descripciones	Mínimo Requerimiento	Exigido
Marca	Especificar	Exigido
Modelo	Especificar	Exigido
Origen	Especificar	Exigido
Cantidad	1 (uno)	Exigido
DESCRIPCIÓN	Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la información perimetral que incluye filtro de paquetes, control de aplicaciones, administración de ancho de banda (QoS), VPN IPSec y SSL, IPS, prevención contra amenazas de virus, spyware y malware Zero Day, bien como controles de transmisión de datos y acceso a internet componiendo una plataforma de seguridad integrada y robusta.	Exigido
	Por plataforma de seguridad se entiende hardware y software integrados de tipo appliance.	Exigido



	La solución tiene que ser ofrecida en alta disponibilidad, se entiende por alta disponibilidad una solución redundante de por lo menos 2 (dos) appliances que cada uno cumpla con las características mínimas mencionadas en estas especificaciones. Si el oferente para poder cumplir con los requerimientos ofrece N appliance, para poder lograr la alta disponibilidad deberá ofertar N * 2 (dos) appliances.	Exigido
	El soporte y licencias ofrecido por el fabricante de la solución tienen que tener vigencia de 3 (tres) años en la modalidad 7x24.	Exigido
	El fabricante debe estar en el cuadrante de líderes de Gartner para Enterprise Firewall o firewalls empresariales en los últimos 5 años.	Exigido
	El fabricante debe estar como líder en el informe de Forrester 2016 para soluciones de protección avanzada.	Exigido
	El fabricante debe estar como líder en el informe de Forrester de Zero Trust eXtended (ZTX) Ecosystem Providers.	Exigido
	El fabricante debe estar certificado para IPv6 en Firewall e IPS por NIST USGv6.	Exigido
	No se aceptarán soluciones UTM ya que estas están orientadas al segmento SMB.	Exigido
	Las características deben ser confirmadas mediante documentación oficial de acceso público (guías de administración, manuales y/o guías técnicas). No se aceptarán documentos generados expresamente para este proceso (ad-hoc).	Exigido
	Las soluciones requeridas deben poder interoperar sin necesidad de software o interacción de terceros.	Exigido
	Las soluciones ofrecidas tienen que ser de un mismo fabricante y tener la posibilidad de orquestarlas entre si y compartir una misma base de inteligencia, se no acepta soluciones que no se orquesten o con bases de firmas de terceras partes.	Exigido
<b>INTERFACES</b>	El equipo debe contar con al menos 4 (cuatro) interfaces de red 100/1.000 RJ45	Exigido
	El equipo debe contar con al menos 8 (ocho) interfaces de red 1 Gbps SFP	Exigido
	Adicionalmente, el equipo deberá contar con un mínimo 2 (dos) interfaces de 1 Gbps (cobre) dedicadas para armar clúster de alta disponibilidad.	Exigido
	1 (una) interface de red 1 Gbps dedicada para administración;	Exigido
	1 (una) interface de tipo consola o similar;	Exigido

	El equipo debe contar con al menos un puerto USB	Exigido
	El equipo debe contar con al menos un puerto Micro USB	Exigido
CAPACIDAD	El equipo debe contar con Throughput de al menos 1.6 Gbps medido con tráfico real (no es válido tomar mediciones ideales o de laboratorio) con la funcionalidad de control de aplicaciones habilitada, para todas las firmas que el fabricante posea actualizadas con la última actualización disponible y log habilitado.	Exigido
	El equipo debe contar con Throughput de al menos 900 Mbps medido con tráfico de real (no es válido tomar mediciones ideales o de laboratorio), con las siguientes funcionalidades habilitadas simultáneamente: Clasificación y control de aplicaciones, IPS, Control de navegación por URL, Antivirus y Antispyware, Control de amenazas avanzadas de día cero (Sandboxing). Para todas las firmas que la plataforma de seguridad posea totalmente activadas, actualizadas al día y con el mayor nivel de seguridad posible; considerando múltiples políticas de seguridad (por lo menos 100 políticas de seguridad aplicadas), y que tengan habilitado la generación de Logs y NAT aplicado a todas las reglas.	Exigido
	El equipo debe soportar al menos 125.000 conexiones simultaneas con todos los módulos de seguridad de capa 7 habilitados simultáneamente, en el mayor nivel de seguridad posible;	Exigido
	El equipo debe soportar al menos 8.500 nuevas conexiones por segundo;	Exigido
	El equipo debe contar con capacidad de descifrado de SSL de al menos 12.000 sesiones simultaneas.	Exigido
	Flujo de ventilación de datacenter del estilo Front-to-back	Exigido
	Ventiladores redundantes.	Exigido
	Se requiere que cada equipo disponga de una disipación de calor máxima de 300 unidades medido en BTU por hora.	Exigido
	El equipo debe contar con Disco Solid State Drive (SSD) de, como mínimo, 240 GB para el sistema y uso de la solución.	Exigido
	El equipo debe soportar al menos 5 (cinco) ruteadores virtuales.	Exigido
	El equipo debe soportar al menos 30 (treinta) zonas de seguridad.	Exigido
	El equipo debe estar licenciado para soportar, sin uso de licenciamiento adicional, 1.000 (mil) clientes de VPN SSL y IPSec simultáneos del estilo cliente-servidor;	Exigido

	El equipo debe estar licenciada para soportar, sin uso de licenciamiento adicional, 2.000 (dos mil) túneles de VPN IPSEC simultáneos del estilo sitio-a-sitio;	Exigido
	Por consola de administración y monitoreo, se entiende el licenciamiento de software necesario para las dos funcionalidades, también como hardware dedicado para el funcionamiento de las mismas.	Exigido
	La consola de administración y monitoreo puede residir en el mismo appliance de seguridad de red, desde que posea recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función;	Exigido
	Para efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados en el site del fabricante como listas de end-of-life y end-of-sale.	Exigido
<b>CARACTERÍSTICAS GENERALES</b>	La solución debe consistir en appliances de seguridad de red con funcionalidades de Next Generation Firewall (NGFW), y consola de administración y monitoreo;	Exigido
	Por funcionalidades de NGFW se entiende: reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos;	Exigido
	La plataforma debe ser optimizada para análisis de contenido de aplicaciones en Capa 7;	Exigido
	El hardware y software que ejecuten las funcionalidades de seguridad de red y de administración y monitoreo, deben ser de tipo appliance. No serán aceptados equipamientos servidores y sistema operacional de uso genérico;	Exigido
	Todos los equipamientos ofrecidos deben ser adecuados para montaje en rack 19	Exigido
	El software deberá ser ofrecido en su versión más estable y/o más avanzada;	Exigido
	La arquitectura de procesadores utilizado por la solución tiene que ser procesadores reprogramables, tipo FPGA, para garantizar que con futuras actualizaciones el equipo no quede obsoleto.	Exigido
	Los dispositivos de seguridad de red deben poseer por lo menos las siguientes funcionalidades:	Exigido
	Soporte de 4094 VLAN Tags 802.1q, tanto por dispositivo como en una sola interfaz;	Exigido
	Agregación de links 802.3ad;	Exigido
	Policy based routing o policy based forwarding;	Exigido
	Ruteo multicast (PIM-SM);	Exigido

DHCP Relay;	Exigido
DHCP Server;	Exigido
Jumbo Frames;	Exigido
Soporte a creación de objetos de red que puedan ser utilizados como dirección IP de interfaces L3;	Exigido
Soportar sub-interfaces ethernet lógicas.	Exigido
Debe soportar los siguientes tipos de NAT:	Exigido
Nat dinámico (Many-to-1);	Exigido
Nat dinámico (Many-to-Many);	Exigido
Nat estático (1-to-1);	Exigido
NAT estático (Many-to-Many);	Exigido
Nat estático bidireccional 1-to-1;	Exigido
Traducción de porta (PAT);	Exigido
NAT de Origen;	Exigido
NAT de Destino;	Exigido
Soportar NAT de Origen y NAT de Destino simultáneamente;	Exigido
Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.	Exigido
Enviar log para sistemas de monitoreo externos, simultáneamente;	Exigido
Debe tener la opción de enviar logs para los sistemas de monitoreo externos vía protocolo TCP y SSL;	Exigido
Debe permitir configurar certificado caso necesario para autenticación del sistema de monitoreo externo de logs;	Exigido

Seguridad contra anti-spoofing;	Exigido
Para IPv4, debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2);	Exigido
Debe soportar MP-BGP	Exigido
Para IPv6, debe soportar enrutamiento estático y dinámico (OSPFv3);	Exigido
Soportar OSPF graceful restart;	Exigido
Debe ser capaz de balancear varios enlaces de internet sin el uso de políticas específicas, permitiendo aplicar una variedad de algoritmos distintos (round Robin, weighted)	Exigido
Soportar BFD (bidirectional forward detection)	Exigido
Soportar LACP/LLDP Pre-negotiation	Exigido
Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPsec, Reglas de seguridad contra DoS (Denial of Service), Descripción SSL y SSH, PBR (Policy Base Routing) o PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, Activo/Activo, Activo/Pasivo, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones;	Exigido
Debe contar con una herramienta para poder optimizar políticas de seguridad, detectar cuáles no se estén usando y por cuánto tiempo; poder aprender de las políticas aplicadas y sugerir que aplicaciones deberían aplicarse a las políticas en el NGFW. Dar estadísticas de uso, ancho de banda por aplicación, último hit de las aplicaciones, sobre cada política, con el objetivo de optimizar y mejorar la configuración del NGFW.	Exigido
El fabricante de la solución ofertada debe contar con una herramienta que convierta desde múltiples fabricantes de firewall (por lo menos: Juniper, Checkpoint, Palo Alto Networks, Cisco, Fortinet, etc) al formato de la solución adquirida, y además optimice las políticas para poder convertir las reglas de origen, destino y puerto en reglas de NGFW basadas en aplicación aprendiendo del tráfico de la red.	Exigido
Los dispositivos de seguridad deben tener la capacidad de operar de forma simultánea mediante el uso de sus interfaces físicas en los siguientes modos dentro del mismo firewall, sin necesidad de tener que hacer uso de contextos virtuales: Modo sniffer (monitoreo y análisis del tráfico de red), Capa 2 (L2), Capa 3 (L3) y modo Transparente;	Exigido
Modo Sniffer, para inspección vía puerto espejo del tráfico de datos de la red;	Exigido
Modo Capa 2 (L2), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación;	Exigido

Modo Capa 3 (L3), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación operando como default Gateway de las redes protegidas;	Exigido
Modo Transparente, para poder inspeccionar de datos en línea y tener visibilidad del control de tráfico en nivel de aplicación sobre 2 puertos en modo bridge/Transparente.	Exigido
Modo mixto de trabajo Sniffer, Transparente, L2 e L3 simultáneamente en diferentes interfaces físicas del mismo equipo;	Exigido
En el modo Transparente, debe poder soportar al menos 256 interfaces (físicas y/o virtuales) sobre cada sistema virtual lógico (Contexto).	Exigido
Soporte a configuración de alta disponibilidad Activo/Pasivo e Activo/Activo:	Exigido
En modo transparente;	Exigido
En layer 3;	Exigido
La configuración en alta disponibilidad debe sincronizar:	Exigido
Sesiones;	Exigido
Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QOS y objetos de red;	Exigido
Certificados de desenscripción;	Exigido
Asociaciones de Seguridad de las VPNs;	Exigido
Tablas FIB;	Exigido
El HA (modo de Alta-Disponibilidad) debe posibilitar monitoreo de fallo de link.	Exigido
Las funcionalidades de control de aplicaciones, VPN IPSec y SSL, QOS, SSL y SSH Decryption y protocolos de enrutamiento dinámico deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.	Exigido
Debe poder inspeccionar protocolos como:	Exigido
GRE	Exigido

CONTROL POR POLÍTICA DE FIREWALL	IPSEC no encriptado (NULL o AH)	Exigido
	GPRS para GTP-U	Exigido
	Deberá soportar controles por zona de seguridad	Exigido
	Controles de políticas por puerto y protocolo.	Exigido
	Control de políticas por aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.	Exigido
	Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad.	Exigido
	Control de políticas por código de País (Por ejemplo: AR, BR, USA, UK, RUS).	Exigido
	Control, inspección y desenscripción de SSL por política para tráfico de entrada (Inbound) y Salida (Outbound).	Exigido
	Debe soportar offload de certificado en inspección de conexiones SSL de entrada (Inbound);	Exigido
	Capacidad de Desenscripción de SSL de al menos 12.000 sesiones simultaneas.	Exigido
	Debe desenscriptar tráfico Inbound y Outbound en conexiones negociadas con TLS v1.1, v1.2 y v1.3;	Exigido
	Debe desenscriptar tráfico que use certificados ECC (como ECDSA)	Exigido
	Control de inspección y desenscripción de SSH por política;	Exigido
	La plataforma de seguridad debe implementar copia del tráfico desenscriptado (SSL y TLS) para soluciones externas de análisis (Forense de red, DLP, Análisis de Amenazas, entre otras);	Exigido
	Se permite el uso de appliance externo, específico para la desenscripción de (SSL y TLS), con copia del tráfico desenscriptado tanto para el firewall, como para otras soluciones de análisis externas.	Exigido

	La solución tiene que contar con un dashboard de reportes y logs dedicados a monitorear el tráfico de descifrado SSL / TLS, este dashboard deberá estar disponible en la interfaz gráfica, con el objetivo de identificar rápidamente problemas relacionados con las técnicas de descifrado de tráfico, el mismo tiene que tener varios estados de troubleshooting y proveer de las herramientas a los administradores para encontrar rápidamente las causas por las cuales se puede producir una falla en la descifrado del tráfico (ej: informar sobre certificados expirados, claves de cifrado débiles, certificados revocados, cierre de la conexión por parte del cliente, entre otros).	Exigido
	Bloqueos de los siguientes tipos de archivos: bat, cab, dll, exe, pif, y reg	Exigido
	Traffic shaping QoS basado en políticas (Prioridad, Garantía y Máximo)	Exigido
	QoS basado en políticas para marcación de paquetes (diffserv marking), inclusive por aplicaciones.	Exigido
	Permitir añadir un comentario de auditoria cada vez que se haga un cambio o se edite la política de seguridad. Cada comentario deberá estar asociado a la versión de la política editada.	Exigido
	Al crear o editar políticas de seguridad, se debe poder forzar el uso de una descripción, tag o comentario de auditoria. Esto con el fin de garantizar buenas prácticas de documentación, organización y auditoria.	Exigido
	Soporte a objetos y Reglas IPV6.	Exigido
	Soporte a objetos y Reglas multicast.	Exigido
	Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.	Exigido
<b>CONTROL DE APLICACIONES</b>	Los dispositivos de seguridad de red deberán poseer la capacidad de reconocer aplicaciones, independiente del puerto y protocolo, con las siguientes funcionalidades:	Exigido
	Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos.	Exigido
	Reconocer por lo menos 2500 aplicaciones diferentes, incluyendo, más no limitado: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail;	Exigido
	Reconocer por lo menos las siguientes aplicaciones: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;	Exigido



Debe inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, incluyendo, más no limitando a RDP en el puerto 80 en vez del 389;	Exigido
Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis comportamental del tráfico observado, incluyendo, más no limitado a Encrypted Bittorrent y aplicaciones VOIP que utilizan cifrado propietario;	Exigido
Identificar el uso de tácticas evasivas, o sea, debe tener la capacidad de visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas vía comunicaciones cifradas, tales como Skype y ataques mediante el puerto 443.	Exigido
Para tráfico Cifrado (SSL y SSH), debe permitir la descifrado de paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante;	Exigido
Debe realizar decodificación de protocolos con el objetivo de detectar aplicaciones encapsuladas dentro del protocolo y validar si el tráfico corresponde con la especificación del protocolo, incluyendo, más no limitado a Yahoo! Instant Messenger usando HTTP. La decodificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación, incluyendo, más no limitado a la compartición de archivos dentro de Webex. También debe detectar el archivo y otros contenidos que deben ser inspeccionados de acuerdo a las Reglas de seguridad implementadas;	Exigido
Debe Identificar el uso de tácticas evasivas vía comunicaciones cifradas;	Exigido
Debe Actualizar la base de firmas de aplicaciones automáticamente;	Exigido
Debe Reconocer aplicaciones en IPv6;	Exigido
Limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD;	Exigido
Los dispositivos de seguridad de red deben poseer la capacidad de identificar al usuario de red con integración al Microsoft Active Directory, sin la necesidad de instalación de agente en el Domain Controller, ni en las estaciones de los usuarios;	Exigido

Debe ser posible adicionar control de aplicaciones en todas las Reglas de seguridad del dispositivo, o sea, no limitándose solamente a la posibilidad de habilitar control de aplicaciones en algunas Reglas;	Exigido
Debe soportar múltiples métodos de identificación y clasificación de las aplicaciones, por lo menos chequeo de firmas, decodificación de protocolos y análisis heurístico;	Exigido
Para mantener la seguridad de la red eficiente, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas;	Exigido
Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interfaz gráfica de la solución, sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones de la empresa;	Exigido
La creación de firmas personalizadas debe permitir el uso de expresiones regulares, contexto (sesiones o transacciones), usando la posición en el payload de los paquetes TCP y UDP y usando decoders de por lo menos los siguientes protocolos:	Exigido
HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP y File body.	Exigido
El fabricante debe permitir la solicitud de inclusión de aplicaciones en la base de firmas de aplicaciones;	Exigido
Debe alertar al usuario cuando una aplicación fuera bloqueada	Exigido
Debe posibilitar que el control de puertos sea aplicado para todas las aplicaciones;	Exigido
Debe posibilitar la diferenciación de tráfico Peer2Peer (Bittorrent, emule, neonet, etc.) proveyendo granularidad de control/políticas para los mismos;	Exigido
Debe posibilitar la diferenciación de tráfico de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) proveyendo granularidad de control/políticas para los mismos;	Exigido
Debe posibilitar la diferenciación y control de partes de las aplicaciones como por ejemplo permitir Gtalk chat y bloquear la transferencia de IM (mensajería instantánea);	Exigido
Debe posibilitar a diferenciación de aplicaciones Proxies (ghostsurf, freegate, etc.) proveyendo granularidad de control/políticas para los mismos;	Exigido
Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como:	Exigido
Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).	Exigido

	Nivel de riesgo de las aplicaciones.	Exigido
	Categoría y sub-categoría de aplicaciones.	Exigido
	Aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda, etc.	Exigido
	Debe poder monitorear aplicaciones SaaS (Software as a service) tanto via GUI como en reporte predefinido.	Exigido
	Las políticas de seguridad tienen que poder ser creadas en base a las aplicaciones y no en base a puertos TCP/UDP.	Exigido
	La aplicación de seguridad debe ser 100% en base a aplicaciones pudiendo aplicar reglas específicas a cada aplicación, ejemplo si dos aplicaciones utilizan el mismo puerto de comunicaciones, se tienen que poder crear 2 políticas de seguridad en las cuales se apliquen controles de seguridad diferentes a cada aplicación.	Exigido
	Al crear políticas basadas en aplicaciones, si las mismas dependen de otras aplicaciones, la interfaz gráfica debe sugerir y permitir agregar las políticas dependientes de la seleccionada, para poder permitir el uso correcto de la aplicación.	Exigido
<b>PREVENCION DE AMENAZAS</b>	Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS, Antivirus y Anti-Spyware integrados en el propio appliance de Firewall	Exigido
	Debe incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware);	Exigido
	Las funcionalidades de IPS, Antivirus y Anti-Spyware deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.	Exigido
	Debe sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo e Activo/pasivo;	Exigido
	Cuando se utilicen las funciones de IPS, Antivirus y Anti-spyware, el equipamiento debe entregar el mismo performance (no degradar) entre tener 1 única firma de IPS habilitada o tener todas las firmas de IPS, Anti-Virus y Antispyware habilitadas simultáneamente.	Exigido
	Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo;	Exigido
	Excepciones por IP de origen o de destino deben ser posibles en las Reglas, de forma general y firma por firma;	Exigido

Debe soportar granularidad en las políticas de IPS Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos esos ítems.	Exigido
Debe permitir el bloqueo de vulnerabilidades.	Exigido
Debe permitir el bloqueo de exploits conocidos.	Exigido
Debe incluir seguridad contra ataques de negación de servicios.	Exigido
Deberá poseer los siguientes mecanismos de inspección de IPS:	Exigido
Análisis de parones de estado de conexiones;	Exigido
Análisis de decodificación de protocolo;	Exigido
Análisis para detección de anomalías de protocolo;	Exigido
Análisis heurístico;	Exigido
IP Defragmentation;	Exigido
Re ensamblado de paquetes de TCP;	Exigido
Bloqueo de paquetes malformados.	Exigido
Ser inmune y capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc;	Exigido
Detectar y bloquear el origen de portscans;	Exigido
Bloquear ataques efectuados por worms conocidos, permitiendo al administrador adicionar nuevos patrones;	Exigido
Soportar los siguientes mecanismos de inspección contra amenazas de red: análisis de patrones de estado de conexiones, análisis de decodificación de protocolo, análisis para detección de anomalías de protocolo, análisis heurístico, IP Defragmentation, re ensamblado de paquetes de TCP y bloqueo de paquetes malformados;	Exigido
Posea firmas específicas para la mitigación de ataques DoS;	Exigido

Posea firmas para bloqueo de ataques de buffer overflow;	Exigido
Posea firmas de C2 (Comando y control) generadas de forma automática.	Exigido
Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.	Exigido
Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3;	Exigido
Soportar bloqueo de archivos por tipo;	Exigido
Identificar y bloquear comunicaciones como botnets;	Exigido
Debe soportar varias técnicas de prevención, incluyendo Drop y tcp-rst (Cliente, Servidor y ambos);	Exigido
Debe soportar referencia cruzada como CVE;	Exigido
La solución ofrecida a partir de los logs debe poder generar indicadores tags para IP de equipos a partir de las detecciones de amenazas con el objetivo de poder utilizar los mismos en grupos dinámicos y aplicarlos a otras políticas. Esta funcionalidad tiene que poder efectuarse localmente en el mismo NGFW o bien poder una vez detectado generar el Tag en un firewall remoto o en la consola de gestión para poder aplicar los grupos dinámicos local, remoto o a todos los NGFW de la organización.	Exigido
La funcionalidad de Indicadores/Tags mencionada en el punto anterior tiene que poder utilizarse para poder agregar o quitar tags a la IP de origen o destino de una detección efectuada.	Exigido
Registrar en la consola de monitoreo las siguientes informaciones sobre amenazas identificadas:	Exigido
Debe soportar la captura de paquetes (PCAP), por firma de IPS y Antispyware;	Exigido
Debe permitir que en la captura de paquetes por firmas de IPS y Antispyware sea definido el número de paquetes a ser capturados. Esta captura debe permitir seleccionar, como mínimo, 50 paquetes;	Exigido
Debe poseer la función resolución de direcciones vía DNS, para que conexiones como destino a dominios maliciosos sean resueltas por el Firewall como direcciones (IPv4 e IPv6), previamente definidos;	Exigido
Permitir el bloqueo de virus, por al menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3;	Exigido

	Los eventos deben identificar el país de donde partió la amenaza;	Exigido
	Debe incluir seguridad contra virus en contenido HTML y JavaScript, software espía (spyware) y worms.	Exigido
	Seguridad contra downloads involuntarios usando HTTP de archivos ejecutables. maliciosos.	Exigido
	Rastreo de virus en pdf.	Exigido
	Debe permitir la inspección en archivos comprimidos que utilizan o algoritmo deflate (zip, gzip, etc.)	Exigido
	Debe ser posible la configuración de diferentes políticas de control de amenazas y ataques basados en políticas del firewall considerando Usuarios, Grupos de usuarios, origen, destino, zonas de seguridad, etc, o sea, cada política de firewall podrá tener una configuración diferente de IPS, siendo esas políticas por Usuarios, Grupos de usuario, origen, destino, zonas de seguridad.	Exigido
	Capacidad de poder redireccionar el tráfico de consultas de DNS a un servidor del tipo sinkhole para poder identificar equipos comprometidos con spyware o actividad de command and control dentro de la red corporativa.	Exigido
<b>ANALISIS DE MALWARE MODERNO</b>	Poseer la capacidad de análisis de amenazas no conocidas;	Exigido
	Debido a los Malware hoy en día se debe ser muy dinámicos y un antivirus común no es capaz de detectar los mismos a la misma velocidad que sus variaciones son creadas, la solución ofertada deber poseer funcionalidades para análisis de Malware no conocidos incluidas en la propia herramienta	Exigido
	El dispositivo de seguridad debe ser capaz de enviar archivos transferidos de forma automática para análisis "In Cloud" o local, donde el archivo será ejecutado y simulado en un ambiente controlado;	Exigido
	Seleccionar a través de la política de Firewall que tipos de archivos sufrirán este análisis;	Exigido
	Soportar el análisis de por lo menos 60 (sesenta) tipos de comportamientos maliciosos para el análisis de la amenaza no conocida;	Exigido
	Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP y Windows 7;	Exigido
	Debe soportar el monitoreo de archivos transferidos por internet (HTTP, FTP, HTTP, SMTP) como también archivos transferidos internamente en los servidores de archivos usando SMB;	Exigido

El sistema de análisis In Cloud o local debe proveer informaciones sobre las acciones del Malware en la máquina infectada, informaciones sobre cuales aplicaciones son utilizadas para causar/propagar la infección, detectar aplicaciones no confiables utilizadas por el Malware, generar firmas de Antivirus y Anti-spyware automáticamente, definir URLs no confiables utilizadas por el nuevo Malware y proveer informaciones sobre el usuario infectado (su dirección ip y su login de red);	Exigido
El sistema automático de análisis "In Cloud" o local debe emitir relación para identificar cuales soluciones de antivirus existentes en el mercado poseen firmas para bloquear el malware;	Exigido
Debe permitir exportar el resultado de los análisis de malware de día Zero en PDF y CSV a partir de la propia interfaz de administración;	Exigido
Debe permitir la descarga de los malware identificados a partir de la propia interfaz de administración;	Exigido
Debe permitir visualizar los resultados de los análisis de malware de día Zero en los diferentes sistemas operacionales soportados;	Exigido
Debe permitir informar al fabricante cuando haya una sospecha de falso-positivo y falso-negativo en el análisis de malware de día Zero a partir de la propia interfaz de administración.	Exigido
Soportar el análisis de archivos ejecutables, DLLs, ZIP y encriptados en SSL en el ambiente controlado;	Exigido
Soportar el análisis de archivos del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), email link, flash, archivos de MacOSX (mach-o, dmg, pkg) y Android APKs en el ambiente controlado;	Exigido
Poseer SLA de, como máximo, 5 minutos para actualización de la base de vacunas contra malware desconocidos identificados en el ambiente controlado;	Exigido
Permitir el envío de archivos para análisis en el ambiente controlado vía web y de forma automática vía API.	Exigido
Debe poder dar veredictos distintos, como minimo:	Exigido
Malicioso	Exigido
Grayware	Exigido
Benigno	Exigido

	Phising	Exigido
	En caso de detectar una forma de evasión de máquina virtual, debe poder enviar de forma automática a revisión en modo Bare Metal (maquinas físicas)	Exigido
	Capacidad de poder aplicar técnicas de aprendizaje de maquina (Machine Learning) localmente sobre los NGFW para poder identificar amenazas desconocidas y bloquear la mismas durante la descarga de los archivos por parte de los usuarios.	Exigido
FILTRO DE URL	La plataforma de seguridad debe poseer las siguientes funcionalidades de filtro de URL	Exigido
	Permite especificar la política por tempo, horario o determinado período (día, mes, año, día de la semana y hora)	Exigido
	Debe ser posible crear políticas por usuario, grupo de usuario, ips, redes y zonas de seguridad	Exigido
	Deberá incluir la capacidad de creación de políticas basadas en la visibilidad y contra de quien está utilizando cual URLs a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, E-Directory y base de datos local	Exigido
	Debe permitir poder publicar los logs de URL con la información de los usuarios conforme a lo descrito en la integración con servicios de directorio	Exigido
	Debe soportar la capacidad de crear políticas basadas en control por URL y categoría URL	Exigido
	Debe bloquear el acceso a sitios de búsqueda (Google, Bing y Yahoo!) en el caso de que la opción de Safe Search este deshabilitada. Debe en ese caso exhibir una página de bloqueo dando instrucciones al usuario de como habilitar dicha función	Exigido
	Debe soportar una cacheé local de URL en el appliance, evitando el delay de comunicación/validación de las URLs	Exigido
	Debe poseer al menos 60 categorías de URLs	Exigido
	Debe soportar la creación de categorías URL custom	Exigido
	Debe soportar la exclusión de URLs del bloqueo por categoría	Exigido
	Debe permitir la customización de la página de bloqueo	Exigido



	Debe permitir o bloquear y continuar (habilitando que el usuario acceso a un sitio potencialmente bloqueado informándole del bloqueo y habilitando el botón de continuar para permitirle seguir a ese site)	Exigido
	Debe soportar la inclusión de los logs del producto de las informaciones de las actividades de los usuarios	Exigido
	Debe evitar la fuga de credenciales desde o hacia sitios web, pudiendo tener granularidad en la configuración, es decir poder permitir o no el uso de credenciales de red internas en diferentes categorías de páginas web (estas categorías podrían ser: phishing, redes sociales, foros, o categorías personalizadas por el cliente, etc), en incluso el uso indebido de los mismos dentro de la red del cliente. El objetivo de este requerimiento es evitar que credenciales internas de la red sean publicadas en sitios de internet, inclusive sitios categorizados como desconocidos por el motor de categorización de filtros de URL.	Exigido
	Debe poder actualizar de forma automática en 5 minutos o menos las categorías de malware, command and control y phishing.	Exigido
	Capacidad de poder aplicar técnicas de aprendizaje de maquina (Machine Learning) localmente sobre los NGFW para poder identificar nuevos sitios de phishing, con la capacidad de poder bloquear los mismos.	Exigido
	Debe contar con multi categorías de URL, que permita que un sitio web pertenezca a dos categorías distintas.	Exigido
<b>IDENTIFICACION DE USUARIOS</b>	Debe incluir a capacidad de creación de políticas basadas en la visibilidad y control de quien está utilizando cuales aplicaciones a través de la integración como servicios de directorio, autenticación vía ldap, Active Directory, E-directory y base de datos local.	Exigido
	Debe poseer integración con Microsoft Active Directory para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.	Exigido
	Debe poseer integración con Radius para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.	Exigido
	Debe poseer integración con TACACS+	Exigido
	Debe posea integración con LDAP para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en Usuarios y Grupos de usuarios.	Exigido
	Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x y soluciones NAC vía syslog, para la identificación de direcciones IP y usuarios	Exigido

	Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal).	Exigido
	Soporte a autenticación Kerberos.	Exigido
	Soporte SAML 2.0	Exigido
	La solución ofrecida debe soportar e incluir múltiples factores de autenticación (como por ejemplo usuario y password + 2FA hard token + 2FA soft token + portal cautivo) para poder utilizarlo tanto en aplicación web como en aplicaciones cliente servidor.	Exigido
	Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que tiene estos servicios	Exigido
	Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en servidores accedidos remotamente, incluso que no sean servidores Windows.	Exigido
QOS	Con la finalidad de controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, (como YouTube, ustream, etc) y tener un alto consumo de ancho de banda, se requiere que la solución, a la vez de poder permitir o negar ese tipo de aplicaciones, debe tener la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones, tanto de audio como de vídeo streaming.	Exigido
	Soportar la creación de políticas de QoS por:	Exigido
	Dirección de origen	Exigido
	Dirección de destino	Exigido
	Por usuario y grupo de LDAP/AD.	Exigido
	Por aplicaciones, incluyendo, más no limitando a Skype, Bittorrent, YouTube y Azureus;	Exigido
	Por puerto;	Exigido
	El QoS debe permitir la definición de clases por:	Exigido
	Ancho de Banda garantizado	Exigido

	Ancho de Banda Máximo	Exigido
	Cola de prioridad.	Exigido
	Soportar priorización Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.	Exigido
	Soportar marcación de paquetes Diffserv, inclusive por aplicaciones;	Exigido
	Disponer de estadísticas Real Time para clases de QoS.	Exigido
	Deberá permitir el monitoreo del uso que las aplicaciones hacen por bytes, sesiones y por usuario.	Exigido
<b>FILTRO DE DATOS</b>	Permite la creación de filtros para archivos y datos predefinidos;	Exigido
	Los archivos deben ser identificados por extensión y firmas;	Exigido
	Permite identificar y opcionalmente prevenir la transferencia de varios tipos de archivos (MS Office, PDF, etc) identificados sobre aplicaciones (P2P, InstantMessaging, SMB, etc);	Exigido
	Soportar la identificación de archivos compactados y las aplicaciones de políticas sobre el contenido de esos tipos de archivos;	Exigido
	Permitir identificar y opcionalmente prevenir la transferencia de informaciones sensibles, incluyendo, más no limitando al número de tarjetas de crédito, permitiendo la creación de nuevos tipos de datos vía expresión regular;	Exigido
	Permitir listar el número de aplicaciones soportadas para control de datos;	Exigido
	Permitir listar el número de tipos de archivos soportados para el control de datos;	Exigido
	Debe poder integrarse con soluciones de punto final de terceros para mejorar la política de DLP.	Exigido
	Debe traer por efecto al menos dos perfiles de bloqueo predefinidos.	Exigido
<b>GEO-LOCALIZACION</b>	Soportar la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sean bloqueados.	Exigido
	Debe posibilitar la visualización de los países de origen y destino en los logs de acceso.	Exigido

	Debe posibilitar la creación de regiones geográficas desde la interfaz gráfica y crear políticas utilizando las mismas.	Exigido
VPN	Soportar VPN Site-to-Site y Cliente-To-Site;	Exigido
	Soportar IPSec VPN;	Exigido
	Soportar SSL VPN;	Exigido
	La VPN IPSEC debe soportar:	Exigido
	DES y 3DES;	Exigido
	Autenticación MD5 e SHA-1;	Exigido
	Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;	Exigido
	Algoritmo Internet Key Exchange (IKEv1 & IKEv2);	Exigido
	AES 128, 192 e 256 (Advanced Encryption Standard)	Exigido
	Debe permitir SSO via Kerberos	Exigido
	Autenticación vía certificado IKE PKI.	Exigido
	Debe ser compatible con la Suite B de protocolos de NSA	Exigido
	Debe poseer interoperabilidad como los siguientes fabricantes:	Exigido
	Cisco;	Exigido
	Checkpoint;	Exigido
	Juniper;	Exigido
	Palo Alto Networks;	Exigido
	Fortinet;	Exigido

Sonic Wall	Exigido
Las VPN SSL deben soportar:	Exigido
Permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operacional del equipamiento o por medio de interfaz WEB;	Exigido
Las funcionalidades de VPN SSL deben ser atendidas con o sin el uso de agente;	Exigido
La asignación de dirección IP en los clientes remotos de VPN;	Exigido
La asignación de DNS en los clientes remotos de VPN;	Exigido
Debe haber la opción de ocultar el agente de VPN instalado en el cliente remoto, tornando el mismo invisible para el usuario;	Exigido
Debe permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN SSL;	Exigido
Las VPN SSL deben soportar proxy arp y el uso de interfaces PPPOE;	Exigido
Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;	Exigido
Permite establecer un túnel VPN client-to-site del cliente a la plataforma de seguridad, proveyendo una solución de single-sign-on a los usuarios, integrándose como las herramientas de Windows-logon;	Exigido
Soporte de lectura y verificación de CRL (certificate revocation list);	Exigido
Permite la aplicación de políticas de seguridad y visibilidades para las aplicaciones que circulan dentro de los túneles SSL;	Exigido
El agente de VPN a ser instalado en los equipamientos desktop y laptops, debe ser capaz de ser distribuido de manera automática vía Microsoft SMS, Active Directory y ser descargado directamente desde su propio portal, en el cual residirá el centralizador de VPN;	Exigido
El agente deberá comunicarse con el portal para determinar las políticas de seguridad del usuario,	Exigido
Debe permitir que las conexiones como VPN SSL sean establecidas de las siguientes formas:	Exigido

	Antes del usuario autenticarse en la estación;	Exigido
	Después de la autenticación del usuario en la estación;	Exigido
	Bajo demanda del usuario;	Exigido
	Deberá mantener una conexión segura con el portal durante la sesión.	Exigido
	El agente de VPN SSL client-to-site debe ser compatible al menos con: Windows XP, Vista, Windows 7, Windows 8, Windows 10, MacOS X;	Exigido
	El portal de VPN debe enviar al cliente remoto la lista de gateways VPN activos para el establecimiento de la conexión, los cuales deben poder ser administrados centralizadamente	Exigido
	Debe haber una opción en el cliente remoto de escoger manualmente el Gateway de VPN y de forma automática a través de la mejor respuesta entre los gateways disponibles con base al más rápido.	Exigido
	Debe poseer la capacidad de identificar el origen de conexión de VPN si es interna o externa	Exigido
<b>CONSOLA DE ADMINISTRACION y MONITOREO</b>	La administración de la solución debe soportar acceso vía SSH, cliente WEB (HTTPS) y API abierta;	Exigido
	En el caso de que sea necesaria la instalación de cliente para administración de la solución, el mismo debe ser compatible con sistemas operacionales Windows y Linux;	Exigido
	La administración debe permitir/hacer:	Exigido
	Creación y administración de políticas de firewall y control de aplicaciones;	Exigido
	Creación y administración de políticas de IPS y Anti-Spyware;	Exigido
	Creación y administración de políticas de filtro de URL	Exigido
	Monitoreo de logs;	Exigido
	Herramientas de investigación de logs;	Exigido
	Debugging;	Exigido

Captura de paquetes.	Exigido
Debe permitir el acceso concurrente de administradores;	Exigido
Debe tener un mecanismo de búsqueda de comandos de administración vía SSH, facilitando la localización de los comandos;	Exigido
Debe permitir usar palabras clave y distintos tags de colores para facilitar la identificación de Reglas;	Exigido
Debe permitir monitorear vía SNMP fallas en el hardware, inserción o remoción de fuentes, discos y ventiladores, uso de recursos por número elevado de sesiones, número de túneles establecidos de VPN cliente-to-site, porcentaje de utilización en referencia al número total soportado/licenciado y número de sesiones establecidas;	Exigido
Debe permitir el bloqueo de alteraciones, en el caso de acceso simultaneo de dos o más administradores;	Exigido
Debe permitir la definición de perfiles de acceso a la consola con permisos granulares como: acceso de escritura, acceso de lectura, creación de usuarios, alteración de configuraciones;	Exigido
Debe permitir la autenticación integrada con Microsoft Active Directory y servidor Radius;	Exigido
Debe permitir la localización de donde están siendo utilizados objetos en: Reglas, dirección IP, Rango de IPs, subredes u objetos	Exigido
Debe poder atribuir secuencialmente un número a cada regla de firewall, NAT, QOS y Reglas de DOS;	Exigido
Debe permitir la creación de Reglas que estén activas en un horario definido;	Exigido
Debe permitir la creación de Reglas con fecha de expiración;	Exigido
Debe poder realizar un backup de las configuraciones y rollback de configuración para la última configuración salvada;	Exigido
Debe soportar el Rollback de Sistema operativo para la última versión local;	Exigido
Debe poseer la habilidad del upgrade vía SCP, TFTP e interfaz de administración;	Exigido
Debe poder validar las Reglas antes de las aplicaciones;	Exigido

Debe permitir la validación de las políticas, avisando cuando haya Reglas que ofusquen o tengan conflicto con otras (shadowing);	Exigido
Debe posibilitar la visualización y comparación de configuraciones actuales, la configuración anterior y configuraciones más antiguas.	Exigido
Debe posibilitar la integración con otras soluciones de SIEM del mercado (third-party SIEM vendors)	Exigido
Debe permitir la generación de logs de auditoria detallados, informando de la configuración realizada, el administrador que la realizo y el horario de la alteración;	Exigido
Deberá tener la capacidad de generar un gráfico que permita visualizar los cambios en la utilización de aplicaciones en la red en lo que se refiere a un período de tiempo anterior, para permitir comparar los diferentes consumos realizados por las aplicaciones en el tiempo presente con relación al pasado;	Exigido
Debe permitir la generación de mapas geográficos en tiempo real para la visualización de orígenes y destinos del tráfico generado en la institución;	Exigido
Debe proveer resúmenes con la vista correlacionada de aplicaciones, amenazas (IPS, Antispyware) URLs y filtro de archivos, para un mejor diagnóstico y respuesta a incidentes;	Exigido
La administración de la solución debe posibilitar la recolección de estadísticas de todo el tráfico que pasa por los dispositivos de seguridad;	Exigido
Debe proveer resúmenes de utilización de los recursos por aplicaciones, amenazas (IPS, Anti-Spyware y antivirus de la solución), etc;	Exigido
Debe proveer de una visualización sumariada de todas las aplicaciones, amenazas (IPS, Antivirus e Anti-Spyware) y URLs que pasan por la solución;	Exigido
Debe poseer un mecanismo "Drill-Down" para navegación por los resúmenes en tiempo real;	Exigido
En las listas de "Drill-Down", debe ser posible identificar el usuario que ha determinado el acceso;	Exigido
Debe ser posible exportar los logs en CSV;	Exigido
Deberá ser posible acceder al equipamiento a aplicar configuraciones durante momentos donde el tráfico sea muy alto y la CPU y memoria del equipamiento este siendo totalmente utilizada.	Exigido



Debe tener rotación de logs;	Exigido
Debe tener presentaciones de las siguientes informaciones, de forma histórica y en tiempo real (actualizado de forma automática y continua cada 1 minuto):	Exigido
Debe mostrar la situación del dispositivo y del cluster;	Exigido
Debe poder mostrar las principales aplicaciones;	Exigido
Debe poder mostrar las principales aplicaciones por riesgo;	Exigido
Debe poder mostrar los administradores autenticados en la plataforma de seguridad;	Exigido
Debe poder mostrar el número de sesiones simultaneas;	Exigido
Debe poder mostrar el estado de las interfaces;	Exigido
Debe poder mostrar el uso de CPU;	Exigido
Generación de reportes. Como mínimo los siguientes reportes deben poder ser generados:	Exigido
Resumen gráfico de las aplicaciones utilizadas;	Exigido
Principales aplicaciones por utilización de ancho de banda de entrada y salida;	Exigido
Principales aplicaciones por tasa de transferencia en bytes;	Exigido
Principales hosts por número de amenazas identificadas;	Exigido
Actividades de un usuario específico y grupo de usuarios del AD/LDAP, incluyendo aplicaciones accedidas y amenazas (IPS, y Anti-Spyware), de red vinculadas a este tráfico;	Exigido
Debe permitir la creación de reportes personalizados;	Exigido
En cada criterio de búsqueda del log debe ser posible incluir múltiples entradas (ej. 10 redes e IP's distintas; servicios HTTP, HTTPS y SMTP), excepto en el campo horario, donde debe ser posible definir un rango de tiempo como criterio de búsqueda;	Exigido
Generar alertas automáticas vía:	Exigido

	Email;	Exigido
	SNMP;	Exigido
	Syslog;	Exigido
	El equipo deberá soportar el envío de logs a un servidor externo syslog según RFC 3164.	Exigido
	La plataforma de seguridad debe permitir a través de API-XML (Application Program Interface) la integración con sistemas existentes en el ambiente de contratación de forma que posibilite que aplicaciones desarrolladas por el cliente puedan interactuar en tiempo real con la solución permitiendo así que Reglas y políticas de seguridad puedan ser modificadas por estas aplicaciones con la utilización de scripts en lenguajes de programación como Perl o PHP.	Exigido
<b>LICENCIAMIENTO</b>	El equipo deberá contar con todas las licencias necesarias para soportar de manera activa todas las prestaciones requeridas en las especificaciones. El plazo de duración de estas licencias será de 3 años (36 meses) al igual que la Garantía.	Exigido
<b>INSTALACION</b>	El proveedor deberá montar apropiadamente en el rack para alojar el appliance, el mismo deberá disponer de todos los accesorios e insumos para la instalación y configuración de toda la solución.	Exigido
<b>SOPORTE</b>	El Oferente adjudicado deberá brindar soporte local tipo 24x7x4.	
<b>GARANTÍA</b>	Cartas de los fabricantes y/o representante oficial donde se especifique una garantía de al menos 3 Años para soporte de atención sobre el Hardware y/o Software, así como también la provisión de repuestos del hardware durante el mismo periodo mencionado.	Exigido
	El soporte de atención debe ser 7x24 con 4 horas de tiempo de respuesta por parte del soporte local para la primera atención, tanto para el hardware como para el software.	Exigido

ITEM 4 SWITCH TOP OF RACK		
Característica	Configuración mínima exigida	Configuración Ofrecida
Marca	Especificar	Exigido
Modelo	Especificar	Exigido
Cantidad	2 (dos)	Exigido

<b>DIMENSIONES DEL EQUIPO</b>	Rack standard compatible con EIA-310D	Exigido
	Formato rackeable, medida en Rack Unit de 1RU como máximo	Exigido
<b>PLATAFORMA</b>	El sistema operativo debe integrarse y ser totalmente administrado desde la solución de orquestación solicitada	Exigido
	El equipo debe soportar un sistema operativo autónomo, así mismo, debe soportar un sistema operativo que permita ser integrado y administrado desde una solución de orquestación SDN. Se requiere que el Switch sea provisto con sistema operativo autónomo.	Exigido
	El sistema operativo de la solución debe soportar procesamiento mutihilo distribuido.	Exigido
	El sistema debe asignar y proteger un espacio de memoria separado a los procesos de features. Los mismos deberán ser instanciados en memoria solo cuando son activados.	Exigido
	Buffer del sistema de al menos 40 MB	Exigido
	Memoria del sistema de al menos 24 GB.	Exigido
	Almacenamiento SSD mínimo de 64 GB	Exigido
<b>INTERFACES</b>	4 (cuatro) Cantidad de puertos QSFP28 40G, habilitados.	Exigido
	El equipo debe contar con 24 (veinticuatro) puertos SFP+ 1/10/25G.	Exigido
	El equipo debe estar equipado con 24 (veinticuatro) puertos SFP+ 1/10/25G adicionales, que podrán ser habilitados con el solo agregado de licencias, permitiendo al equipo llegar a 48 puertos SFP+ 1/10/25G habilitados.	Exigido
	Todos los puertos SFP+ 1/10/25G deberán soportar Fiber Channel 16G con el solo agregado de licencias.	Exigido
	Se debe proveer con el equipo 6 (seis) cables preensamblados con conectores para SFP+ 10GE, de al menos 3 metros de longitud.	Exigido
	Se debe proveer con el equipo 4 (cuatro) Transceivers 10G SR.	Exigido

PERFORMANCE DEL SISTEMA	El equipo debe contar con 2 (dos) interfaces de management, al menos uno debe ser óptico SFP.	Exigido
	El equipo debe contar con al menos un puerto serial	Exigido
	El equipo debe contar con al menos un puerto USB 2.0	Exigido
	Ancho de banda no bloqueante (non blocking) de al menos 3,5 Tbps	Exigido
	Capacidad de forwarding de al menos 2,5 bpps	Exigido
	Debe soportar al menos 4000 VLANs	Exigido
	Debe soportar al menos 250.000 MAC Address	Exigido
	Debe soportar al menos 1.000 entradas NAT	Exigido
	Debe soportar al menos 30.000 rutas multicast	Exigido
	Debe soportar al menos 800.000 entradas IP	Exigido
	Debe soportar al menos 800.000 rutas LPM	Exigido
	Debe soportar al menos 30.000 grupos IGMP	Exigido
	Debe soportar al menos 8.000 entradas ACL de ingreso	Exigido
	Debe soportar al menos 4.000 entradas ACL de egreso	Exigido
	Debe soportar al menos 60 caminos ECMP	Exigido
	Debe soportar al menos 500 puertos agregados	Exigido
	Debe soportar al menos 30 enlaces en un puerto agregado	Exigido
	Debe soportar al menos 4 sesiones de puertos espejos	Exigido
	Debe soportar al menos 3000 VLANs en instancias RPTST	Exigido

PROTOCOLOS Y FUNCIONALIDADES	Debe soportar al menos 60 instancias MST	Exigido
	Debe soportar al menos 450 grupos de VRRP (o similar)	Exigido
	NTP Debe ser capaz de soportar NTP para sincronizar su propio reloj interno, así como para propagar dicha información a otros dispositivos en la red o a través del fabric.	Exigido
	Debe ser capaz de soportar IPv6 e IPv6 routing.	Exigido
	IGMP, IGMP Snooping.	Exigido
	Multicast routing, PBR	Exigido
	PIM, PIM-SSM	Exigido
	Túneles GRE	Exigido
	Soporte de AAA, Radius, TACACS+.	Exigido
	Soporte de Jumbo Frame (9000+ MTU)	Exigido
	IEEE 802.1AB (LLDP)	Exigido
	IEEE_802.1p	Exigido
	Debe soportar 802.1q VLAN tagging / trunking.	Exigido
	IEEE_802.1x	Exigido
	IEEE_802.1s	Exigido
	IEEE_802.1w	Exigido
	IEEE_802.3	Exigido
	IEEE 802.3i	Exigido
	IEEE_802.3u	Exigido

IEEE_802.3ab	Exigido
IEEE_802.3ad	Exigido
IEEE_802.3x	Exigido
Class of Service (CoS)	Exigido
Differentiated Services Code Point (DSCP)	Exigido
El sistema deberá permitir habilitar Fiber Channel y Fiber Channel over Ethernet con el solo agregado de licencias.	Exigido
El sistema deberá permitir habilitar FCoE NPV con el solo agregado de licencias.	Exigido
Deberá implementar un mecanismo prevención de la dispersión del dominio ID y reducir el tamaño de la tabla FCF.	Exigido
Debe soportar puertos ruteados.	Exigido
Debe soportar manejo de listas de permisos en puertos físicos y virtuales.	Exigido
Debe soportar: BGP, GRE, IS-IS, MSDP, OSPF, PBR, PIM, SSM, VRF, VXLAN BGP EVPN, SRv6 (no EVPN), and SR-MPLS (no EVPN)	Exigido
Debe soportar: ruteo estático, VRF-Lite, VRRP, BFD, BFD, DHCP Relay.	Exigido
Debe soportar diferentes implementacion de funcionalidades de telemetría, como Sflow, FTE, SSX o similares)	Exigido
Debe soportar PTP	Exigido
Deberá soportar SR-MPLS, con el solo agregado de licencias.	Exigido
Deberá soportar EVPN-VXLAN Multi-Site con el solo agregado de licencias.	Exigido
Debe soportar MPLS Layer 3 VPN con el solo agregado de licencias.	Exigido

	Compatibilidad con 802.1D.	Exigido
	Soporte multichassis link aggregation (MLAG) o similar	Exigido
	El sistema debe permitir implementar MACSec con el solo agregado de licencias.	Exigido
<b>MTBF</b>	El equipo deberá contar con un MTBF superior a 360.000 horas.	Exigido
<b>NORMAS Y CERTIFICACIONES DE SEGURIDAD Y EMISIONES</b>	EN 60950-1	Exigido
	IEC 60950-1	Exigido
	UL 60950-1	Exigido
	EN 55022 Class A	Exigido
	EN61000-3-3	Exigido
	EN61000-3-2	Exigido
	EN 55024	Exigido
	EN 300386	Exigido
	RoHS-6	Exigido
<b>ALIMENTACIÓN ELÉCTRICA</b>	El equipo debe funcionar con un voltaje entrante en el rango de 100-240 VAC a 50-60 Hz.	Exigido
	Deberá incluir los accesorios necesarios para montar en racks estándar de 19.	Exigido
	No se aceptarán transformadores de 220VCA a 110VCA agregados a la fuente integrada en el equipo. Dicha fuente debe aceptar directamente 220VCA 50 hz. No se aceptarán fuentes externas.	Exigido
	El equipo debe contar con al menos dos fuentes de alimentación AC trabajando en manera redundante, con la posibilidad de extracción e intercambio en línea (HOT SWAP) sin que afecte el funcionamiento del equipo y sin necesidad de apagarlo.	Exigido

<b>REFRIGERACIÓN</b>	La circulación de aire del equipo debe ser Front to Back.	Exigido
<b>ACCESORIOS</b>	Los accesorios requeridos para entregar el equipo en perfecto estado de operación (software, power cord, rackmount kit. )	Exigido
<b>LICENCIAMIENTO</b>	El equipo deberá contar con todas las licencias necesarias para soportar de manera activa todas las prestaciones requeridas en las especificaciones. El plazo de duración de estas licencias será de 3 años (36 meses) al igual que la Garantía.	Exigido
<b>INSTALACION</b>	El proveedor deberá montar apropiadamente en el rack para alojar el appliance, el mismo deberá disponer de todos los accesorios e insumos para la instalación y configuración de toda la solución.	Exigido
<b>GARANTÍA</b>	Cartas de los fabricantes y/o representante oficial donde se especifique una garantía de al menos 3 Años para soporte de atención sobre el Hardware y/o Software, así como también la provisión de repuestos del hardware durante el mismo periodo mencionado.	Exigido
	El soporte de atención debe ser 7x24 con 4 horas de tiempo de respuesta por parte del soporte local para la primera atención, tanto para el hardware como para el software.	Exigido

#### **GENERALIDADES**

**Personal proveído por DNVS:** DNVS asignará el personal técnico del Dpto. de Informática, que supervisará todo el ciclo de ejecución de lo contratado, en coordinación con el personal asignado por el Proveedor como contrapartida.

**Infraestructura proveída por DNVS:** El Dpto. de Informática proporcionará al Proveedor el lugar y las estaciones de trabajo requeridas para la ejecución de las tareas necesarias para la provisión de bienes y ejecución de servicios asociados. Se utilizarán normas, modelos y procedimientos estándares recomendados por el Dpto. de Informática.

**Recepción Provisoria:** La recepción provisoria de los sistemas y/o equipos, formalizada mediante el Acta de Recepción Provisoria, se emitirá en la fecha en que se reciban la totalidad de los sistemas y/o equipos adjudicados debidamente instalados.

**Recepción Definitiva:** La recepción definitiva de los sistemas y/o equipos, formalizada mediante el Acta de Recepción Definitiva, se realizará posterior a la fecha de suscripción del Acta de Recepción Provisoria, siempre que se haya constatado el estricto cumplimiento de la oferta del Proveedor y del Pliego de Bases y Condiciones, y sea comprobada la buena calidad y correcto funcionamiento de los sistemas y/o equipos proveídos e instalados a satisfacción del Banco Central del Paraguay. Al efecto, el Proveedor deberá ejecutar una serie de pruebas de correcto funcionamiento de los sistemas y/o equipos proveídos, de acuerdo a las recomendaciones del fabricante y respecto a las funcionalidades requeridas en el Pliego de Bases y Condiciones.

En caso de existir fallas o divergencias con las características de los sistemas y/o equipos ofertados respecto a los entregados o su instalación esta recepción se efectuará después de subsanarse los defectos y/o divergencias presentadas.

Las Actas de Recepción Provisoria y Definitiva deberán ser firmadas por el Proveedor y los representantes del área técnica de la DNVS encargada de la verificación técnica de los sistemas y/o equipos entregados e instalados y el Dpto. de Informática.

**Soporte técnico, actualizaciones y garantía:** Se deberá brindar el soporte técnico y la garantía del fabricante de los sistemas y/o equipos proveídos (hardware y software), el servicio de actualizaciones de software para los mismos ante nuevas versiones o parches de seguridad de la solución, así como el soporte técnico del fabricante para el escalamiento y apertura de casos, sin costo extra, a partir de la fecha de la Recepción Definitiva, bajo la modalidad de atención 7x24x365 ante fallas, nuevos requerimientos de configuración que puedan surgir y/o ajustes del sistema y/o necesidades de acompañamiento técnico, con posibilidad de escalamiento directo al fabricante.

El Proveedor deberá disponer de los canales de solicitud habilitados para el soporte, consistentes en dos números de contacto y cuentas de correo electrónico. En ese sentido, el Proveedor una vez adjudicado, deberá detallar los siguientes datos: Nombres y apellidos, cargos, correos corporativos y números de teléfono de línea fija y móvil.



Se deberá cubrir el soporte de atención de Hardware/Software, Mano de Obra y Repuestos (dicha garantía deberá cubrir el reemplazo por cualquier daño del equipo o componentes internos, los cuales deberán ser sustituidos). Si la reparación implicará la indisponibilidad del equipo por 24 hs. o más, el Proveedor suministrará en préstamo otro equipo de características similares mientras dure la reparación del mismo. El soporte de atención debe ser 7x24x365 y la Mano de Obra y Repuestos deberán estar incluidos. Los tiempos de respuestas, resoluciones de problemas, cambios de partes y niveles de criticidad se definen en el Acuerdo de Nivel de Servicio descripto más adelante en este apartado.

La garantía y soporte técnico deberá incluir la posibilidad de acceso directo al Centro Asistencial del fabricante para resolución o apertura de casos mientras dure el soporte solicitado. Será un requisito indispensable que el Oferente esté autorizado por el fabricante a prestar el servicio técnico y el cambio de partes por garantía. Además, se deberá incluir la revisión, backup, actualización y verificación a pedido de la DNVS, acerca del funcionamiento periódico de todo el Hardware/Software proveídos y los cambios de elementos/partes que así lo requieran. A fin de que dichas tareas no interfieran en el desarrollo de las actividades de la DNVS, quedará a cargo del personal técnico del BCP definir el momento de ejecución de estas tareas.

Los plazos de vigencia se detallan a continuación:

- Item 1, 2, 3 y 4: por un periodo mínimo de 3 (tres) años a partir de la Recepción Definitiva. Con posibilidad de extender la garantía a costa de la DNVS por 2 (dos) años más.

Además, el Proveedor deberá proveer repuestos sin costo para la DNVS, en caso de fallas por defectos de fabricación y/o instalación por el periodo citado. Asimismo, deberá asegurar la comercialización de repuestos para los equipos y/o sistemas proveídos como mínimo durante los 2 (dos) años posteriores al vencimiento del plazo de soporte técnico y garantía del fabricante.

**Acuerdo de Nivel de Servicio:** El Proveedor suscribirá un acuerdo de nivel de servicio (ANS o SLA por sus siglas en inglés) relacionado a cuanto sigue:

Los plazos para atención a solicitudes de asistencia técnica se determinarán de acuerdo al grado de criticidad y conforme a la severidad de problemas. Estos se clasifican según su grado de severidad de acuerdo a la siguiente tabla, la definición respecto al nivel de criticidad será determinado exclusivamente por LA dnvs en la solicitud de soporte:

Los plazos para atención a solicitudes de asistencia técnica se determinarán de acuerdo al grado de criticidad y conforme a la severidad de problemas. Estos se clasifican según su grado de severidad de acuerdo a la siguiente tabla, la definición respecto al nivel de criticidad será determinado exclusivamente por LA dnvs en la solicitud de soporte.

Niveles de Problemas	Descripción
Crítico	Los incidentes críticos son aquellos que afectan severamente al hardware, appliances y/o software provisto, la capacidad o despacho, los cargos y la capacidad de procesamiento de datos. Los problemas críticos requieren acciones correctivas inmediatas, sin importar la hora o el día en que se produzcan, como por ejemplo una falla total del hardware y/o software, degradación del funcionamiento del hardware/software.
No críticos	Los incidentes menores son problemas que no se consideran críticos o mayores. Un problema menor puede tener impacto en uno o en un número limitado de funcionalidades del hardware y/o software. Los incidentes menores no dañan significativamente el funcionamiento de los sistemas, ni afectan significativamente a los servicios. Estos problemas son tolerables durante el uso de los equipos y software.

El Proveedor deberá dar cumplimiento estricto a los Niveles de Compromisos en relación al Soporte Técnico de Acuerdo de Nivel de Servicio (SLA) que se detalla a continuación:

Acuerdo de Nivel de Servicio (SLA) del Soporte Técnico	
Soporte Técnico	Nivel de Servicio

Nivel de Criticidad		Crítico	No Crítico
Tiempo disponible para el servicio		7x24x365	7x24x365
Resolución de Fallas	Tiempo de respuesta al BCP	≤30 min.	≤90 mins.
	Tiempo de reposición del equipo, appliance, software o resolución de la falla.	4 h.	24 h
Idiomas disponibles para el servicio		Español o Inglés	

El Proveedor no podrá alegar inconvenientes del fabricante para la obtención de los servicios mencionados, debiendo garantizar en toda circunstancia la posibilidad de escalamiento de los eventos de soporte o problemas con el hardware y/o software.

Se deberá emitir un informe al finalizar la intervención y/o resolución de problemas para ayudar a la gestión que tiene revisiones periódicas del historial de incidentes del sistema y rendimiento de los servicios de todo el hardware y software provisto.

Ante cada notificación el Proveedor deberá realizar y presentar a la DNVS un informe que contendrá como mínimo la siguiente información: Descripción detallada del problema, su causa y solución propuesta, personal que se asignó a la resolución del mismo, problemas que se presentaron durante la resolución, documentación de los cambios realizados, recomendaciones, fecha y hora de resolución.

**Compatibilidad:** Todos los equipos ofertados deben de ser totalmente compatibles en todas sus funcionalidades con los componentes, equipos y dispositivos requeridos para los demás lotes de acuerdo a las especificaciones técnicas detallados para los mismos. Así mismo toda la solución ofertada debe ser totalmente compatible con los servicios, configuraciones y aplicaciones existentes actualmente en Producción en la infraestructura de la DNVS, para lo cual el Oferente deberá asistir a la visita técnica prevista para el presente llamado.

**Configuración, integración, instalación y puesta a punto:** El Proveedor deberá proporcionar los servicios completos de configuración avanzada, además proveer los servicios de integración con los demás dispositivos de redes, servidores y aplicaciones que sean ofertados en el presente llamado, conforme a las funcionalidades requeridas en las especificaciones técnicas de cada equipo y/o appliance. La configuración deberá cumplir con las políticas y normas de seguridad informática de la Red Institucional de la DNVS. La modalidad del servicio de configuración e integración requerido es llave en mano y deberá ser adecuada a la infraestructura existente de la DNVS. El servicio contemplará el suministro, actividades de montaje, instalación en general, configuración y puesta en funcionamiento de servidores y equipos en el lugar indicado por la DNVS. Los sistemas, equipos, appliances y software solicitados son de funcionamiento independiente pero integrados. Sin embargo, si ante un reclamo de la DNVS respecto a una falla de integración, y en el caso de que se adjudiquen la provisión e instalación de cada uno de los equipos a diferentes Proveedores, alguno de éstos dudase de su obligación de solucionarla respecto al equipo proveído por el mismo, el área técnica administradora del contrato solicitará un informe a ambos Proveedores y se reserva el derecho de analizar dichos informes, realizar las verificaciones técnicas que correspondan y decidir unilateralmente cuál Proveedor será responsable de brindar la solución que corresponda.

Se entiende por integración y puesta a punto, a los requerimientos técnicos de interoperabilidad y configuraciones (tanto básicas, como avanzadas) detallados en las especificaciones técnicas de equipos y/o appliances. Por lo tanto, la definición de estos requerimientos técnicos y niveles de integración, serán determinados exclusivamente por el equipo técnico de la DNVS, de acuerdo a las funcionalidades requeridas en las especificaciones técnicas de los equipos y/o appliances, y el Proveedor deberá encargarse de ejecutar los trabajos, adecuaciones y/o provisión necesaria de licencias para cumplir con dichos requerimientos, sin costo extra alguno para la DNVS. De este modo de la DNVS podrá solicitar que sean realizadas todas las configuraciones y/o integraciones (de acuerdo a las especificaciones técnicas) que considere apropiadas y necesarias para la correcta implementación de la infraestructura (requerimientos de seguridad, servicios, máquinas virtuales, funcionalidades, migraciones, respaldos automáticos, optimizaciones, etc) que será migrada en los nuevos equipos y/o appliances a ser provistos.

Cualquiera de los requerimientos de configuración, integración, instalación y puesta a punto expuestos anteriormente podrán ser solicitados durante todo el periodo de soporte técnico especificado para cada Lote.

**Capacitación:** Una vez entregados e instalados los sistemas y/o equipos contratados, el Proveedor deberá brindar una

capacitación integral (teórica y práctica) a los funcionarios de la DNVS encargados de operar los mismos, respecto al modo de uso, funcionalidades, ajustes, etc.; de al menos 48 (cuarenta y ocho) horas para todos los ítems, en las fechas y horario a definir conjuntamente entre el Proveedor y la DNVS. La capacitación se debe iniciar en un periodo no mayor a 90 (noventa) días luego de la recepción provisoria de los equipos, appliance o software. El contenido de la capacitación deberá incluir tópicos sobre los siguientes sistemas y/o equipos provistos:

- Instalación y configuración de los equipos, appliances y software proveídos.
- Arquitectura de funcionamiento de todos equipos, appliances y software proveídos.
- Configuración básica y avanzada de plataforma y software relacionado por cada equipo, appliance y software proveídos.
- Diagrama de conexiones físicas y lógicas principales.
- Resolución de problemas frecuentes.
- Administración de funciones de software de gerenciamiento con casos prácticos y ejemplos de configuraciones frecuentes.
- Instalación de los sistemas operativos de los equipos y las configuraciones necesarias para brindar diferentes servicios y ampliaciones.
- Operar los equipos realizando tareas de monitoreo, pruebas y ajustes en servicios necesarios para mantener el sistema en condiciones de operación normal.
- Mantener el equipamiento en su estado operacional nominal a través de un programa de mantenimiento preventivo y correctivo.
- Instrucciones y procedimientos para mantenimientos de emergencia.

#### **Instalación, Cableado, Conectores, Accesorios y Canalizaciones y/o Ductos:**

La instalación y configuración de los sistemas y/o equipos quedará a cargo del Proveedor de cada ítem adjudicado.

El cableado, conectores y accesorios deberán cumplir con las normas internacionales estándar para este tipo de instalaciones y deberán ser provistos en su totalidad por el Proveedor de cada ítem adjudicado.

Cuando la instalación de los sistemas y/o equipos requiera o afecte de alguna forma la estructura existente del datacenter, se deberá prever la reposición dejando la estructura en perfecto estado; de igual manera, en caso de que sea requerido algún tipo de obra civil estas quedarán a cargo del Proveedor de cada ítem adjudicado. Además, en caso de que los sistemas y/o equipos a ser instalados requieran canalizaciones y/o ductos adicionales a los existentes en la obra, los materiales y accesorios requeridos para estos quedarán a cargo del Proveedor de cada Lote adjudicado.

La instalación de las conexiones eléctricas necesarias para correcto el funcionamiento de los sistemas y/o equipos quedará a cargo del Proveedor y se deberán incluir en caso de ser necesarios, conductores eléctricos, accesorios, ductos, canalizaciones, tableros, bandejas metálicas, etc; es decir todo para la puesta en funcionamiento de los sistemas y/o equipos. Todo el cableado deberá estar correctamente etiquetado, ordenado y documentado de acuerdo al diagrama de conexiones físicas a ser entregado por el Proveedor, una vez finalizados los trabajos de instalación.

**Accesorios de Instalación e integración:** para los ítems del 1 al 4, cada Proveedor de cada ítem adjudicado será responsable de la entrega de todos los accesorios requeridos para instalar e integrar los equipos en perfecto estado de operación. (Módulos Ópticos, software, patch cords, power cord, rackmount kit, etc.). La falta de algún elemento (hardware, software y/o cualquier componente o partes) necesario para el funcionamiento de lo contratado, tanto individualmente, o como en operación conjunta, para los fines funcionales previstos por la Contratante, originado por cualquier tipo de interpretación de las especificaciones técnicas, obligará al Proveedor a proveerlo de inmediato y sin cargo adicional para la Contratante. Las adecuaciones que fueran necesarias realizar para dar cumplimiento a lo establecido precedentemente serán realizadas por la Contratante en coordinación con cada Proveedor y garantizando en todos los casos la preservación de la funcionalidad requerida.

**Condición de equipos:** Los equipos deben ser nuevos y de última generación para la familia de equipos ofertados. No se aceptarán equipos usados, reacondicionados y/o refurbished.

**Licenciamiento:** se registrará de acuerdo a los requerimientos individuales de cada equipo, appliance y/o software exigidos.

Cada equipo y/o appliance ofertado debe incluir en su totalidad las licencias necesarias para cumplir las funciones y características exigidas la Sección III. Además, para todos los ítems, la entrega de cualquier Software significará la entrega de las Licencias de Uso del Software, emitidas a nombre de la DNVS, como mínimo durante el periodo que dure la garantía, es decir se deberá presentar, luego de la provisión, un documento del fabricante que certifique que las licencias fueron registradas a nombre de la DNVS.

**Compromiso de Confidencialidad:** El personal interviniente del Proveedor deberá firmar un Compromiso de Confidencialidad de la Información, dado que dicho personal podría acceder a información confidencial de la Contratante.

La firma del Compromiso de Confidencialidad se realizará posterior a la suscripción del contrato.

En caso que se incorporen otros funcionarios o empleados del Proveedor, la Dirección Administrativa de la DNVS será la encargada de gestionar la firma del Compromiso de Confidencialidad por parte de los mismos.

#### **Lugar y Otras Condiciones:**

- La implementación debe realizarse en los centros de datos Primario y Secundario de la DNVS.

- Todos los trabajos, deberán ser realizados en las oficinas de la DNVS, y en horario laboral ordinario de la institución, comprendido entre las 7:00 a 15:00 horas. Para servicios fuera de estos horarios deberá ser comunicado en cada caso el ingreso o permanencia del personal técnico, por nota dirigida al Jefe del Dpto. de Informática con al menos 24 horas de antelación de producida la necesidad de la prestación del servicio fuera del horario arriba especificado.

#### Responsabilidades del Proveedor:

1. Contar con la cantidad de personal técnico especializado necesario para realizar la instalación de los sistemas y/o equipos contratados en el plazo establecido, así como solucionar cualquier situación que se presente con los mismos. En los casos que por cualquier motivo el personal habilitado no pudiere asistir y el Proveedor lo deba sustituir por otro, el mismo deberá también ajustarse a los requerimientos de la DNVS y ser previamente habilitado en la nómina de personal acreditado para la ejecución del servicio solicitado.
2. Será responsabilidad del Proveedor nombrar por escrito a una persona encargada, la cual deberá informar diariamente sobre el avance de la ejecución de los trabajos de instalación al funcionario a ser designado por el Dpto. de Informática.
3. Es responsabilidad del Proveedor proporcionar a su personal de todas las herramientas y accesorios necesarios para realizar sus tareas, teniendo en cuenta todas las normas de seguridad requeridas para este tipo de trabajo.
4. Presentar un cronograma semanal de las entregas e instalación que realizará, el cual servirá de base para el control a ser efectuado por el funcionario designado del Dpto. de Informática. El primer cronograma semanal deberá ser entregado dentro del plazo de 5 (cinco) días hábiles posteriores a la suscripción del Contrato.
5. Proveer al final del proyecto de la implementación de cada ítem, toda la documentación de lo proveído, se entiende por estas documentaciones al conjunto de literaturas técnicas para la instalación, operación, funcionamiento, detección y prevención de fallas, condiciones de uso de lo proveído; e instalación, explotación, operación y solución de fallas. En todos los casos deberá proveer al menos una copia material de la documentación (impresa y en CD-ROM/DVD).
6. Proporcionar al final del proyecto de la implementación de cada ítem, la documentación de operación básica y avanzada de los sistemas y/o equipos proveídos, así como también los diagramas de bloque de los sistemas, diagramas de cableado detallado, plano del Datacenter con el cableado utilizado para cada sistema y manuales de operación de los equipos. También se deberá proveer documentación o guía de operación y verificación de la utilización en conjunto de los sistemas requeridos, esta documentación deberá ser elaborada por el Proveedor al final del proyecto en idioma español y deberá contener los detalles técnicos y diagramas asociados a cada sistema y equipo en la solución, incluyendo escenarios de utilización, configuración de los equipos y resolución de problemas. En todos los casos deberá proveer al menos una copia material de la documentación (impresa y en CD-ROM/DVD). A manera de guía, citamos brevemente las documentaciones a elaborar y a entregar a la GTIC:
  - a. Descripción de la Ingeniería de la Red y equipos.
  - b. Planos de vista general de la Red y de los equipos a utilizar con su identificación.
  - c. Planos de ubicación de los equipos.
  - d. Diagrama de conexión de los Equipos de Comunicación, físico y lógico, describiendo el Protocolo con que se conectan (L2, L3, etc.), y los IP´s involucrados de los Equipos, red, etc. (IP planning).
  - e. Otros planos que sean necesarios para la administración de la Red, para el seguimiento de cableado que faciliten los trabajos de mantenimiento.
  - f. Manual de cada dispositivo utilizado en la implementación de la red.
  - g. Diagrama de conexiones físicas y posiciones de equipos en los racks.
7. Luego de la finalización de la implementación y despliegue de todo el proyecto se deberá proporcionar la documentación detallada con todos los pasos realizados durante el proceso de instalación, configuración e integración de lo proveído. En caso de surgir problemas durante la integración y/o despliegue, los mismos deberán ser registrados y documentadas las soluciones. En todos los casos deberá proveer al menos una copia material de la documentación (impresa y en CD-ROM/DVD).

## Identificación de la unidad solicitante y justificaciones

- Ing. Marcos León, Jefe del Dpto. de Informática.
- El proceso licitatorio referente al proyecto de reingeniería de la infraestructura tecnológica, que se sustenta principalmente en las recomendaciones realizadas por la OPS en el *Plan Integral de desarrollo de tecnología para la DNVS*, tendientes a la certificación de la DNVS como Autoridad Regulatoria de Referencia otorgada por la Organización Panamericana de la Salud.

Es importante mencionar que el MSP y BS ha concretado un *ACUERDO ESPECIFICO DE COOPERACION PARA LA IMPLEMENTACION DEL SISTEMA INFORMÁTICO INTEGRADO DE GESTION DE REGISTROS SANITARIOS Y ESTABLECIMIENTOS REGULADOS POR EL MINISTERIO DE SALUD PÚBLICA Y BIENESTAR SOCIAL A TRAVÉS DE LA DINAVIS*, que tiene como objetivo la

digitalización de los procesos para la obtención del Registro Sanitario y habilitación de establecimientos regulados por la Ley 1119/97, hecho sumamente importante para la modernización, transparencia y eficiencia de nuestros procesos.

La implementación de trámites de manera electrónica permitirá a la DNVS ofrecer: a) Mejor servicio al usuario y ciudadano, simplificando y facilitando su vinculación con la Autoridad Sanitaria mediante la utilización de las Tecnologías de la Información y las Comunicaciones (TICs), a fin de reducir los tiempos y costos involucrados en los trámites administrativos. b) Mejor gestión pública, perfeccionando la calidad de los procedimientos y sistemas de información, con el objetivo de lograr una administración pública eficaz y transparente. c) Reducción de costos, utilizando todas las potencialidades de las TICs para simplificar los procedimientos internos de la DNVS y de interacción entre esta y el usuario. d) Mayor Transparencia, facilitando el acceso de los habitantes y ciudadanos a la información pública mediante su página web institucional. Asimismo, la implementación de los trámites de forma electrónica facilita el acercamiento de la administración pública a los usuarios, ya que permite la operación desde sus propios establecimientos, reduciendo así las necesidades de traslados y tiempos de esperas, así como la limitación que representan los horarios de funcionamiento administrativo.

Así mismo es importante traer a colación que mediante Ley N° 6524/2020 Que declara Estado emergencia en todo el territorio de la Republica del Paraguay ante la pandemia declarada por la Organización Mundial de la Salud a causa del COVID-19 o Coronavirus y se establecen medidas administrativas, fiscales y financieras; y de conformidad al Artículo 2° autoriza al Poder Ejecutivo a implementar medidas excepcionales para fortalecer el sistema de salud entre otros.

En ese mismo sentido, el Decreto N° 3442/2020, dispone la implementación de acciones preventivas ante el riesgo de expansión del Coronavirus (COVID-19) al territorio nacional, conforme al Plan Nacional de Respuesta a Virus Respiratorios 2020, aprobado por resolución del Ministerio de Salud Pública y Bienestar Social, por lo que corresponde a las dependencias públicas impulsar la implementación y mejorar los procesos para poder realizarlos de forma digital y remota.

En ese sentido, se ha realizado el relevamiento y la sistematización de las necesidades tecnológicas requeridas para la actualización tecnológica, que comprende de unos Smart Data Center ubicado en el edificio de la DNVS, así como la seguridad, cómputo, almacenamiento y comunicaciones que brindan el soporte actualmente a las aplicaciones de la DNVS. Dicho relevamiento fue elaborado en base a una infraestructura tolerante a fallos, que cuenta con: servidores, equipos de comunicación, almacenamiento distribuido, almacenamiento compartido, equipos de seguridad avanzados, software de virtualización y administración centralizada de toda la arquitectura a ser adquirida, el cual también contempla la adquisición de hardware y software asociados.

Así mismo es importante mencionar que actualmente se encuentra en proceso de ejecución la cooperación realizada por IESC (*International Executive Service Corps*), acordada a través de la Carta de Colaboración (CdC) firmada entre el MSP y BS y la IESC en el marco de del Programa T-FAST financiado por el USDA en Paraguay.

Esta cooperación consiste en proveer a la DNVS de una solución de cómputo, basada en una plataforma de escritorios virtuales en busca de la provisión de una solución de virtualización de aplicaciones y escritorios, con infraestructura informática para la Dirección Nacional de Vigilancia Sanitaria.

Para complementar las cooperaciones recibidas, corresponde a la DNVS llevar adelante la implementación de un proyecto de reingeniería de la infraestructura tecnológica y en ese sentido el departamento de informática ha solicitado los precios referenciales a diferentes Empresas, en base a lo necesitado y teniendo en cuenta la dependencia tecnológica que deriva de dicha operación.

- La planificación se trata de un llamado sucesivo.
- El proyecto de Reingeniería de la infraestructura de cómputo ha sido desarrollado por el área de tecnología de la DNVS en el que se comprende; 1 (un) Datacenter ubicados en edificio de la DNVS, así como toda la infraestructura de seguridad, cómputo, almacenamiento y comunicaciones que brindan el soporte actualmente a las aplicaciones de la DNVS.

A tal efecto fueron elaboradas las especificaciones técnicas para la adquisición de una infraestructura tolerante a fallos, que comprende: Solución Hiperconvergente, Equipos de Comunicaciones, Equipos de Seguridad Avanzados, Hardware y Software de Backup, Antivirus, Licenciamiento Microsoft y Racks Autónomos.

Las especificaciones técnicas exigidas, van acorde a las tecnologías ya instaladas en el marco de cooperación de la IESC, T-FAST y demás y bajo estos criterios nos encontramos dentro de una dependencia tecnológica.

## 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:

Ítem	Descripción del bien	Cantidad	Unidad de medida	Lugar de entrega de los bienes	Fecha(s) final(es) de entrega de los bienes
1	<i>Racks Inteligentes</i>	2	<i>Unidad</i>	<i>Edificio de la DNVS (Iturbe 883 casi Manuel Domínguez)</i>	<i>90 (noventa) días, contados a partir de la suscripción del Contrato.</i>
2	Sistema de cómputo Hiperconvergencia para virtualización de Servidores	1	<i>Unidad</i>	<i>Edificio de la DNVS (Iturbe 883 casi Manuel Domínguez)</i>	<i>90 (noventa) días, contados a partir de la suscripción del Contrato.</i>
3	Equipos de Seguridad (Next generation Firewall)	1	<i>Unidad</i>	<i>Edificio de la DNVS (Iturbe 883 casi Manuel Domínguez)</i>	<i>90 (noventa) días, contados a partir de la suscripción del Contrato.</i>
4	EQUIPOS DE RED (SWITCHES ToR)	2 (dos)	<i>Unidad</i>	<i>Edificio de la DNVS (Iturbe 883 casi Manuel Domínguez)</i>	<i>120 (ciento veinte) días, contados a partir de la suscripción del Contrato.</i>

## 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:

*Al culminar los trabajos de instalación para la entrega final, los funcionarios del Dpto. de Informática procederán a realizar las inspecciones y verificaciones de los equipos instalados y el funcionamiento correcto, luego se emitirá Acta de Conformidad acerca de lo realizado.*

1. El proveedor realizará todas las pruebas y/o inspecciones de los Bienes, por su cuenta y sin costo alguno para la contratante.
2. Las inspecciones y pruebas podrán realizarse en las instalaciones del Proveedor o de sus subcontratistas, en el lugar de entrega y/o en el lugar de destino final de entrega de los bienes, o en otro lugar en este apartado.  
  
Cuando dichas inspecciones o pruebas sean realizadas en recintos del Proveedor o de sus subcontratistas se le proporcionarán a los inspectores todas las facilidades y asistencia razonables, incluso el acceso a los planos y datos sobre producción, sin cargo alguno para la contratante.
3. La contratante o su representante designado tendrá derecho a presenciar las pruebas y/o inspecciones mencionadas en la cláusula anterior, siempre y cuando éste asuma todos los costos y gastos que ocasione su participación, incluyendo gastos de viaje, alojamiento y alimentación.
4. Cuando el proveedor esté listo para realizar dichas pruebas e inspecciones, notificará oportunamente a la contratante indicándole el lugar y la hora. El proveedor obtendrá de una tercera parte, si corresponde, o del fabricante cualquier permiso o consentimiento necesario para permitir al contratante o a su representante designado presenciar las pruebas o inspecciones.
5. La contratante podrá requerirle al proveedor que realice algunas pruebas y/o inspecciones que no están requeridas en el contrato, pero que considere necesarias para verificar que las características y funcionamiento de los bienes cumplan con los códigos de las especificaciones técnicas y normas establecidas en el contrato. Los costos adicionales razonables que incurra el proveedor por dichas pruebas e inspecciones serán sumados al precio del contrato, en cuyo caso la contratante deberá justificar a través de un dictamen fundado en el interés público comprometido. Asimismo, si dichas pruebas y/o inspecciones impidieran el avance de la fabricación y/o el desempeño de otras obligaciones del proveedor bajo el contrato, deberán realizarse los ajustes correspondientes a las Fechas de Entrega y de Cumplimiento y de las otras obligaciones afectadas.
6. El proveedor presentará a la contratante un informe de los resultados de dichas pruebas y/o inspecciones.
7. La contratante podrá rechazar algunos de los bienes o componentes de ellos que no pasen las pruebas o inspecciones o que no se ajusten a las especificaciones. El proveedor tendrá que rectificar o reemplazar dichos bienes o componentes rechazados o hacer las modificaciones necesarias para cumplir con las especificaciones sin ningún costo para la contratante. Asimismo, tendrá que repetir las pruebas o inspecciones, sin ningún costo para la contratante, una vez que notifique a la contratante.
8. El proveedor acepta que ni la realización de pruebas o inspecciones de los bienes o de parte de ellos, ni la presencia de la contratante o de su representante, ni la emisión de informes, lo eximirán de las garantías u otras obligaciones en virtud del contrato.

---

## Indicadores de Cumplimiento

El documento requerido para acreditar el cumplimiento contractual, será:

Planificación de indicadores de cumplimiento:

INDICADOR	TIPO	FECHA DE PRESENTACIÓN PREVISTA (se indica la fecha que debe presentar según el PBC)
<i>Nota de Remisión</i>	<i>Acta de recepción</i>	<i>Diciembre 2021</i>

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

## Criterios de Adjudicación

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

1. La adjudicación en los procesos de contratación en los cuales se aplique la modalidad de contrato abierto, se efectuará por las cantidades o montos máximos solicitados en el llamado, sin que ello implique obligación de la convocante de requerir la provisión de esa cantidad o monto durante de la vigencia del contrato, obligándose sí respecto de las cantidades o montos mínimos establecidos.
2. En caso de que la convocante no haya adquirido la cantidad o monto mínimo establecido, deberá consultar al proveedor si desea ampliarlo para el siguiente ejercicio fiscal, hasta cumplir el mínimo.
3. Al momento de adjudicar el contrato, la convocante se reserva el derecho a disminuir la cantidad de bienes requeridos, por razones de disponibilidad presupuestaria u otras razones debidamente justificadas. Estas variaciones no podrán alterar los precios unitarios u otros términos y condiciones de la oferta y de los documentos de la licitación.

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



## Notificaciones

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

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

## Audiencia Informativa

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

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

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

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

## Documentación requerida para la firma del contrato

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

### 1. Personas Físicas / Jurídicas

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

- Certificado de no hallarse en interdicción judicial expedido por la Dirección General de Registros Públicos;

- Constancia de no adeudar aporte obrero patronal expedida por el Instituto de Previsión Social;

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

- En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para asumir todas las obligaciones emergentes del contrato hasta su terminación;

- Certificado de cumplimiento tributario vigente a la firma del contrato.

## 2. Documentos. Consorcios

- Cada integrante del consorcio que sea una persona física o jurídica deberá presentar los documentos requeridos para oferentes individuales especificados en los apartados precedentes.

- Original o fotocopia del consorcio constituido.

- Documentos que acrediten las facultades del firmante del contrato para comprometer solidariamente al consorcio.

- En el caso que suscriba el contrato otra persona en su representación, acompañar poder suficiente del apoderado para asumir todas las obligaciones emergentes del contrato hasta su terminación.

# CONDICIONES CONTRACTUALES

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

## Interpretación

### Interpretación

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

### 2. Condiciones prohibidas, inválidas o inejecutables

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

### 3. Limitación de Dispensas:

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

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

## Subcontratación

El porcentaje permitido para la subcontratación será de:

No Aplica

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

## Derechos Intelectuales

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

2. Sujeto al cumplimiento por parte de la contratante del párrafo siguiente, el proveedor indemnizará y liberará de toda responsabilidad

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

- a) La instalación de los bienes por el proveedor o el uso de los bienes en la República del Paraguay; y
- b) La venta de los productos producidos por los bienes en cualquier país.

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

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

4. Si el Proveedor no notifica a la Contratante dentro de treinta (30) días a partir del recibo de dicha comunicación de su intención de proceder con tales procesos o reclamos, la Contratante tendrá derecho a emprender dichas acciones en su propio nombre.

5. La Contratante se compromete, a solicitud del proveedor, a prestarle toda la asistencia posible para que el proveedor pueda contestar las citadas acciones legales o reclamaciones. La Contratante será reembolsada por el proveedor por todos los gastos razonables en que hubiera incurrido.

6. La Contratante deberá indemnizar y eximir de culpa al proveedor y a sus empleados, funcionarios y subcontratistas, por cualquier litigio, acción legal o procedimiento administrativo, reclamo, demanda, pérdida, daño, costo y gasto, de cualquier naturaleza, incluyendo honorarios y gastos de abogado, que pudieran afectar al proveedor como resultado de cualquier transgresión o supuesta transgresión de patentes, modelos de aparatos, diseños registrados, marcas registradas, derechos de autor, o cualquier otro derecho de propiedad intelectual registrado o ya existente a la fecha del Contrato, que pudieran suscitarse con motivo de cualquier diseño, datos, planos, especificaciones, u otros documentos o materiales que hubieran sido suministrados o diseñados por la Contratante o a nombre suyo.

---

## Transporte

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

Si 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 cuando se trate de un solo sobre. Cuando se trate de dos sobres la confidencialidad de la primera etapa será hasta la emisión del acto administrativo de selección de ofertas técnicas, reanudándose la confidencialidad después de la apertura en público de las ofertas económicas hasta la emisión de la Resolución de adjudicación.

2. La Contratante y el Proveedor deberán mantener confidencialidad y en ningún momento divulgarán a terceros, sin el consentimiento de la otra parte, documentos, datos u otra información que hubiera sido directa o indirectamente proporcionada por la otra parte en conexión con el Contrato, antes, durante o después de la ejecución del mismo. No obstante, el proveedor podrá proporcionar a sus subcontratistas los documentos, datos e información recibidos de la contratante para que puedan cumplir con su trabajo en virtud del contrato. En tal caso, el proveedor obtendrá de dichos subcontratistas un compromiso de confidencialidad similar al requerido al proveedor en la presente cláusula.

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

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

a) La contratante o el proveedor requieran compartir con otras instituciones que participan en el financiamiento del Contrato;

b) Actualmente o en el futuro se hace de dominio público sin culpa de ninguna de las partes;

c) Puede comprobarse que estaba en posesión de esa parte en el momento que fue divulgada y no fue previamente obtenida directa o indirectamente de la otra parte; o

d) Que de otra manera fue legalmente puesta a la disponibilidad de esa parte por un tercero que no tenía obligación de confidencialidad.

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

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

---

## **Obligatoriedad de declarar información del personal del contratista en el SICP**

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

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

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

4. La Contratante podrá realizar las diligencias que considere necesarias para verificar que la totalidad de las personas que prestan servicios personales en relación de dependencia para la contratista y eventuales subcontratistas se encuentren debidamente individualizados en los listados recibidos.

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

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

---

## **Formas y condiciones de pago**

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

1. Documentos Genéricos:

1. Nota de remisión;

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:

El pago se realizará con créditos presupuestarios del Ejercicio Fiscal 2021 para el Sub Objeto de Gasto. El pago se solicitará por Nota, a ser presentada en la Ventanilla Única de Proveedores de la Dirección de Administración y Finanzas, donde se procederá en forma inmediata en el Sistema Administrativo Financiero, adjuntando para el efecto la Factura, Acta de Recepción, Orden de Servicio Original, Certificado de cumplimiento tributario, fotocopia de la Resolución de Adjudicación, fotocopia del contrato vigente y adenda si las hubiere.

A los efectos de este contrato en aplicación del Art. De la Ley 3439/07 De Contrataciones Públicas se retendrá el 0,5% sobre el importe de cada factura, deducido los impuestos correspondientes.

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:

La fórmula y procedimiento para el cálculo de reajustes serán los siguientes: Siempre y cuando la variación del IPC publicado por el BCP haya sufrido una variación igual o mayor al quince por ciento (15%) referente a la fecha de apertura de ofertas, conforme a la siguiente formula:

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

Dónde:

*Pr:* Precio Reajustado.

*P:* Precio adjudicado.

*IPC1:* Índice de precios al Consumidor publicado por el Banco Central del Paraguay, correspondiente al mes de la provisión del servicio.

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

*No se reconocerán pedidos de reajuste de precios si la provisión se encuentra atrasada.*

*La adjudicada deberá presentar por escrito su pedido a la Convocante, dentro de los 5 (cinco) días hábiles posteriores a la fecha de publicación por parte del BCP de los datos sobre la variación del IPC; adjuntado toda la documentación respaldatoria para justificar su pretensión. Fenecido dicho plazo, no se admitirán pedidos de reajustes.*

## 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:

0,01 %

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:

0,001

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

Si la Contratante no efectuara cualquiera de los pagos al proveedor en las fechas de vencimiento correspondiente o dentro del plazo

establecido en la presente cláusula, la Contratante pagará al proveedor interés sobre los montos de los pagos morosos a la tasa establecida en este apartado, por el período de la demora hasta que haya efectuado el pago completo, ya sea antes o después de cualquier juicio.

### Impuestos y derechos

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

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

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

No Aplica

### Convenios Modificatorios

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

1. Cuando el sistema de adjudicación adoptado sea de abastecimiento simultáneo las ampliaciones de los contratos se registrarán por las disposiciones contenidas en la Ley N° 2051/2003, sus modificaciones y reglamentaciones, que para el efecto emita la DNCP.
2. Tratándose de contratos abiertos, las modificaciones a ser introducidas se registrarán atendiendo a la reglamentación vigente.
3. La celebración de un Convenio 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 N° 2051/03 "De Contrataciones Públicas", de la ley N° 1879/02 "De arbitraje y mediación" y las condiciones del Contrato. El procedimiento arbitral se llevará a cabo ante el Centro de Arbitraje y Mediación del Paraguay (en adelante, "CAMP"). El tribunal estará conformado por tres árbitros designados de la lista del cuerpo arbitral del CAMP, que decidirá conforme a derecho, siendo el laudo definitivo y vinculante para las partes. Se aplicará el reglamento respectivo y demás disposiciones que regule dicho procedimiento al momento de ser requerido, declarando las partes conocer y aceptar los vigentes, incluso en orden a su régimen de gastos y costas, considerándolos parte integrante del presente Contrato. Para la ejecución del laudo arbitral, o para dirimir cuestiones que no sean arbitrables, las partes se someterán a la jurisdicción de los tribunales de la ciudad de Asunción, República del Paraguay".

## Fraude y Corrupción

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

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

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

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

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

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

Fraude y corrupción comprenden actos como:

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

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

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

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

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

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

# MODELO DE CONTRATO

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

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

# FORMULARIOS

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

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

