DOCUMENTO DE LICITACION

Instituto Hondureño de Seguridad Social

LICITACIÓN PÚBLICA NACIONAL
LPN 026-2018

"Adquisición de Solución de Comunicación Core Firewall Interno, Switches de Acceso, Certificación y Reparación de Fibra Óptica, Solución de Seguridad Perimetral de Próxima Generación y Solución de Comunicación de Telefonía IP para el IHSS"

Fuente de Financiamiento:

Fondos Propios del IHSS

Tegucigalpa, octubre *de 2018*

INDICE

SECCION I - INSTRUCCIONES A LOS OFERENTES

IO-01 CONTRATANTE

El Instituto Hondureño de Seguridad Social (IHSS), promueve la Licitación Pública ***026- 2018***, que tiene por objeto la "Adquisición de Solución de Comunicación Core Firewall Interno, Switches de Acceso, Certificación y Reparación de Fibra Óptica, Solución de Seguridad Perimetral de Próxima Generación, Solución de Comunicación de Telefonía IP para el IHSS".

IO-02 TIPO DE CONTRATO

Como resultado de esta licitación se podrá otorgar un contrato de suministro de servicios para la "Adquisición de Solución de Comunicación Core Firewall Interno, Switches de Acceso, Certificación y Reparación de Fibra Óptica, Solución de Seguridad Perimetral de Próxima Generación, Solución de Comunicación de Telefonía IP para el IHSS".

IO-03 OBJETO DE CONTRATACION

Esta contratación tiene como objeto contar con la Solución de Comunicación Core Firewall Interno, Switches de Acceso, Certificación y Reparación de Fibra Óptica, Solución de Seguridad Perimetral de Próxima Generación, Solución de Comunicación de Telefonía IP para el IHSS".

IO-04 IDIOMA DE LAS OFERTAS

Deberán presentarse en español.

IO-05 PRESENTACIÓN DE OFERTAS

Las ofertas se presentarán en: Lobby, primer piso del Edificio Administrativo, Barrio Abajo, Tegucigalpa, M.D.C.

El día de presentación de ofertas será el día **lunes 10 de diciembre** de 2018

La hora límite de presentación de ofertas será hasta las: 10:00 am, hora oficial

APERTURA DE OFERTAS

La apertura de las ofertas se realizará en el auditórium, 11 piso del Edificio Administrativo, Barrio Abajo, Tegucigalpa, M.D.C.

El día de apertura de ofertas será **lunes 10 de diciembre** de 2018

La hora de apertura de ofertas será a las: 10:15 am, hora oficial

IO-06 VIGENCIA DE LAS OFERTAS

Las ofertas deberán tener una vigencia mínima de noventa (90) días calendarios contados a partir de la fecha de presentación de ofertas.

IO-07 GARANTIA DE MANTENIMIENTO DE OFERTA

La oferta deberá acompañarse de una Garantía de Mantenimiento de Oferta por un valor del dos por ciento (2%) del valor total de la oferta.

Se aceptarán solamente fianzas y garantías bancarias emitidas por instituciones debidamente autorizadas, cheques certificados y bonos del Estado representativos de obligaciones de la deuda pública, que fueren emitidos de conformidad con la Ley de Crédito Público.

La garantía deberá tener una vigencia de 30 días calendarios, posteriores a la fecha de presentación de las ofertas. **Por lo que la garantía será de 120 días calendarios a partir de la fecha de presentación de ofertas.**

IO-08 PLAZO DE ADJUDICACION

La adjudicación del contrato al licitante ganador, se dará dentro de los ***noventa días calendario*** contados a partir de la fecha de presentación de las ofertas.

IO-09 DOCUMENTOS A PRESENTAR

Cada oferta deberá incluir los siguientes documentos, en caso de ser copias estos deberán presentarse autenticados:

09.1 Información Legal

1. Copia legible y autenticada del Instrumento Público de Constitución de la Sociedad Mercantil y sus reformas, inscrita en el Registro de la Propiedad de Inmueble y Mercantil, respectivo.
2. Fotocopia autenticada del Poder de Representación de la Sociedad Mercantil
3. Fotocopia legible de la tarjeta de identidad del Representante Legal del oferente.
4. Fotocopia legible del RTN de la Sociedad Mercantil y su Representante Legal.

5. La Garantía de Mantenimiento de la Oferta, del dos por ciento (2%) del monto de la oferta.
6. Constancia de solvencia vigente a la fecha de apertura, extendida por la Alcaldía Municipal del domicilio del oferente y su Representante Legal.
7. Declaración Jurada (original y autenticada) del Oferente y su Representante Legal de no estar comprendido en ninguno de las inhabilidades a los que se refiere la Ley de Contratación del Estado en sus artículos 15 y 16.
8. Carta de la oferta firmada y sellada por el representante legal de la empresa.
9. Permiso de Operación vigente y/o constancia de que está en trámite, extendida por la Alcaldía Municipal del domicilio de la empresa.
10. Constancia de inscripción en el Registro de Proveedores y Contratistas del Estado, extendida por la ONCAE y/o constancia de que está en trámite la misma. De no tenerla se deberá presentará a la firma del contrato.
11. Certificación de la Secretaria de Desarrollo Económico indicando que la Empresa es distribuidor y/o representante de los equipos para los lotes 1,2,4 y 5.

09.2 Información Financiera

a) Constancias de Institución Bancaria acreditada en el país, en donde conste que tiene cuentas de ahorro o de cheques que acrediten un saldo promedio (de los últimos 6 meses) no menor al 10 % del monto de la oferta y / o línea de crédito de institución bancaria por un monto no menor al 20% del monto de la oferta.

b) Estados Financieros Auditados de los años 2016 y 2017 por un afirma auditora independiente, auditor externo, o contador colegiado.

09.3 Información idoneidad Técnica

El oferente deberá presentar junto con su oferta los siguientes documentos de Idoneidad técnica:

a) Declaración Jurada de calidad y prontitud del servicio a proveer y del cumplimiento de las Especificaciones y condiciones Técnicas establecidas por el IHSS, asimismo soporte y disponibilidad del servicio en un 99.9% debidamente autenticada.

b) El Oferente deberá proporcionar evidencia documentada que demuestre su experiencia en la prestación de los servicios que presta, por lo cual deberá de presentar copia de tres (3) Contratos o constancias, de los últimos cinco (5) años de servicio o bienes similares, además debe de adjuntar los datos teléfono, dirección y persona contacto.

c) El oferente deberá entregar para los lotes 1, 2, 4 y 5 nota del fabricante de la solución donde se indique que esta cuenta con la capacidad técnica y el respaldo de la marca y del fabricante para el tipo de implementación de productos y servicios descritos en los lotes anteriores.

d) Los oferentes deberán entregar copia de los currículos vitae del personal técnico que estará realizando las actividades para los diferentes lotes, donde se pueda validar la capacidad técnica del recurso humano, deberá acreditarlo con los certificados extendidos a cada uno de ellos.

09.4 Información Económica

- Cuadro de presentación de la oferta. La propuesta económica deberá contener la descripción de los servicios con sus precios unitarios y totales, debidamente firmados y sellados por el representante legal de la empresa.
- Lista de Precios, en la siguiente forma: El Oferente completará estos formularios de Listas de Precios de acuerdo con las instrucciones indicadas. La lista de servicios en la columna 1 de la Lista de Precios.

LISTA DE PRECIOS

LOTE	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
1	**ADQUISICION DE EQUIPO DE COMUNICACIONES SWITCH CORE PARA EL CENTRO DE DATOS DEL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL**		
	Equipo de comunicaciones integrado que incluye:		
	a) Componente de comunicaciones modular de clase empresarial tipo switch CORE		
	b) Componente de seguridad interna (NGFW).		
	c) Componente de administración y monitoreo		
	Servicio de Instalación, configuración, pruebas, verificación del correcto funcionamiento de la solución de infraestructura, equipos, componentes y su software de gestión, incluyendo los Accesorios, patchcords, medios, equipos, software, etc que sean necesarios para la instalación y puesta en producción del equipo.		

	Servicio de Capacitación por parte del representante del fabricante en el uso, administración, configuración y monitoreo de la solución adquirida para el Área de Infraestructura de la Gerencia de IT del IHSS, para ocho personas un mínimo		
	Servicio de Soporte Técnico por un año para toda la solución		
	Servicios de Suscripción con el fabricante por un año: el equipo deberá contar con una suscripción para descarga de archivos de definiciones de manera automática para todos los componentes de la solución, la cual deberá incluir soporte técnico (local y remoto cuando fuera necesario), actualizaciones y corrección de errores		
	TOTAL LOTE 1 (Componentes, Servicios y Accesorios)		
2	**EQUIPOS SWITCHES DE ACCESO PARA LA RED LAN DEL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL**		
	Equipos		
	Servicios de instalación y configuración		
	Servicio de Soporte Técnico por un año		
	TOTAL LOTE 2 (Componentes, Servicios y Accesorios)		
3	**CERTIFICACION Y REPARACION DE CABLEADO DE FIBRA OPTICA (BACKBONE) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL**		
	Suministro de patchcords de fibra óptica		
	Diagnóstico de los enlaces de fibra óptica que incluya la validación de capacidades de cada línea y la limpieza de gabinetes, conectores y adaptadores actualmente instalados.		
	Servicio de Reparación de fibra óptica		
	Servicio de Certificación de fibra óptica		
	TOTAL LOTE 3 (Insumos, Servicios y Accesorios)		
4	**SOLUCION DE FIREWALL DE SEGURIDAD PERIMETRAL DE PROXIMA GENERACION PARA EL**		

	INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL		
	Equipo de seguridad perimetral integrado que incluye:		
	a) Componente de seguridad perimetral		
	b) Componente de Administración y monitoreo		
	Servicio de Instalación, configuración, pruebas, verificación del correcto funcionamiento de la solución de infraestructura, equipos, componentes y su software de gestión, incluyendo los accesorios, medios, equipos, etc que sean necesarios para la instalación y puesta en producción del equipo.		
	Servicio de Capacitación por parte del representante del fabricante en el uso, administración, configuración y monitoreo de la solución adquirida para el Área de Infraestructura de la Gerencia de IT del IHSS, para seis personas un mínimo.		
	Servicios de Suscripción con el fabricante por un año: el equipo deberá contar con una suscripción para descarga de archivos de definiciones de manera automática para todos los componentes de la solución, la cual deberá incluir soporte técnico (local y remoto cuando fuera necesario), actualizaciones y corrección de errores.		
	TOTAL LOTE 4 (Componentes, Servicios y Accesorios)		
5	**ADQUISICION E INSTALACIÓN DE UNA SOLUCION DE COMUNICACIONES TELEFONICA IP DE CLASE EMPRESARIAL PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL**		
	3 equipos de comunicación telefónica IP, que incluye:		
	a) Componente de Comunicaciones de Telefonía IP		
	b) Componente de administración y monitoreo		
	Servicio de Instalación, configuración, pruebas, verificación del correcto funcionamiento de la solución de infraestructura, equipos, componentes y su software de gestión;		

	incluyendo todos los accesorios, medios, equipos, etc que sean necesarios para la puesta en producción del equipo.		
	Servicio de Capacitación por parte del representante del fabricante o representante en el uso, administración, configuración y monitoreo de la solución adquirida para el Área de Infraestructura de la Gerencia de IT del IHSS, para ocho personas un mínimo.		
	Servicio de Soporte técnico (local y remoto cuando fuera necesario), actualizaciones y corrección de errores.		
	TOTAL LOTE 5 (Componentes, Servicios y Accesorios)		
	GRAN TOTAL		

Nombre del Oferente *[indicar el nombre completo del Oferente]* Firma del Oferente *[firma de la persona que firma la Oferta]* Fecha *[Indicar Fecha]*

Este listado deberá ser firmado y sellado por el representante

legal del ofertante. Los precios deberán presentarse en Lempiras

y únicamente con dos decimales.

El valor total de la oferta no deberá comprender el impuesto sobre ventas, ya que **El IHSS ESTA EXENTO DE PAGO DE IMPUESTOS, según Resolución Nº DGCFA-ISV 0002-2018**.

IO-10 ACLARACIONES

Toda empresa que de manera oficial haya obtenido los documentos de licitación que requiera alguna aclaración deberá comunicarse con el comprador por escrito a la dirección que éste facilita. El Comprador responderá por escrito a todas las solicitudes de aclaración, siempre que dichas solicitudes las reciba el Comprador por lo menos **15 días** calendarios antes de la fecha límite para la presentación de ofertas. El Comprador enviará copia de las respuestas, incluyendo una descripción de las consultas realizadas, sin identificar su fuente, a todos los que hubiesen adquirido los Documentos de Licitación directamente del Comprador.
Para consultas o información dirigirse a la Subgerencia de Suministros, Materiales y
Compras, 6 pisos edificio administrativo Barrio Abajo Tegucigalpa M.D.C

Las respuestas a solicitudes de aclaración se publicarán además en el Sistema de Información de Contratación y Adquisiciones del Estado de

Honduras, "HonduCompras", (www.honducompras.gob.hn).

Si como resultado de las aclaraciones, el Comprador considera necesario enmendar los Documentos de Licitación, deberá hacerlo siguiendo el procedimiento establecido para el mismo.

Toda enmienda emitida formará parte íntegra de los Documentos de Licitación y deberá ser comunicada por escrito a todos los que hayan obtenido los documentos de Licitación directamente del Comprador.

Las enmiendas a documentos de licitación se publicarán además en el Sistema de Información de Contratación y Adquisiciones del Estado de Honduras, "HonduCompras", (www.honducompras.gob.hn).

IO-11 EVALUACION DE OFERTAS.

Las ofertas serán evaluadas de acuerdo a la siguiente rutina de fases acumulativas:

11.1 FASE I, Verificación Legal

Cada uno de los aspectos a verificar será de cumplimiento obligatorio:

ASPECTO VERIFICABLE	CUMPLE	NO CUMPLE
1) Copia legible y autenticada del Instrumento Público de Constitución de la Sociedad Mercantil y sus reformas, inscrita en el Registro de la Propiedad de Inmueble y Mercantil, respectivo.		
2) Fotocopia autenticada del Poder de Representación de la Sociedad Mercantil		
3) Fotocopia legible autenticada de la tarjeta de identidad del Representante Legal del oferente		
4) Fotocopia legible autenticada del RTN de la Sociedad Mercantil y su Representante Legal.		
5) La Garantía de Mantenimiento de la Oferta, del dos por ciento (2%) del monto de la oferta.		
6) Constancia de solvencia vigente a la fecha de apertura, extendida por la Alcaldía Municipal del domicilio del oferente y su Representante Legal		
7) Declaración Jurada (original y autenticada) del Oferente y su Representante Legal de no estar comprendido en ninguno de las inhabilidades a los que se refiere la Ley de Contratación del Estado en sus artículos 15 y 16.		
8) Carta de la oferta original firmada y sellada por el representante legal de la empresa.		

9) Permiso de Operación vigente, extendida por la Alcaldía Municipal del domicilio de la empresa. En caso de presentar copia esta deberá autenticarse.		
10) Certificación o constancia extendida por CONATEL que está autorizado para brindar los servicios que oferta.		
11) Constancia de inscripción en el Registro de Proveedores y Contratistas del Estado, extendida por la ONCAE y/o constancia de que está en trámite la misma. De no disponer de este documento deberá presentarse a la firma del contrato.		

11.2 FASE II, Evaluación Financiera

ASPECTO VERIFICABLE	CUMPLE	NO CUMPLE
a) Constancias de Institución Bancaria acreditada en el país, en donde conste que tiene cuentas de ahorro o de cheques que acrediten un saldo promedio (de los últimos 6 meses) no menor al 10 % del monto de la oferta y / o línea de crédito de institución bancaria por un monto no menor al 20% del monto de la oferta.		
b) Estados Financieros Auditados de los años 2016 y 2017 por una firma auditora independiente, auditor externo o contador colegiado.		

11.3 FASE III, Evaluación Técnica

11.3.1 Sub Fase III.A Evaluación Técnica en Documentos:

ASPECTO EVALUABLE EN DOCUMENTOS OFICIALES	CUMPLE	NO CUMPLE
a) Declaración Jurada de calidad y prontitud del servicio a proveer y del cumplimiento de las Especificaciones y condiciones Técnicas establecidas por el IHSS, asimismo soporte y disponibilidad del servicio en un 99.9% debidamente autenticada.		
b) El Oferente deberá proporcionar evidencia documentada que demuestre su experiencia en la prestación de los servicios que presta, por lo cual deberá de presentar copia de al menos tres (3) Contratos o Constancias de servicios Similares, de los últimos cinco (5) años, además debe de adjuntar los datos teléfono, dirección y persona contacto.		

11.3.2 Sub Fase III B Evaluación técnica Física (NO APLICA)

De la muestra de ***[insertar detalle y tamaño mínimo de muestra requerida]***, ***[insertar número***

ASPECTO VERIFICABLE	CUMPLE	NO CUMPLE
La Carta de Oferta firmada por el representante legal de la empresa.		
La Lista de precios, firmada por el representante legal de la empresa.		

de unidades que serán sometidas a ensayos] unidades serán sometidos cada uno de ellos a la siguiente batería secuencial de ensayos físicos: NO APLICA

Ensayo 1: ***[insertar detalle de ensayo a realizar]*** Ensayo 2: ***[insertar detalle de ensayo a realizar]*** Ensayo 3: ***[insertar detalle de ensayo a realizar]*** Ensayo 4: ***[insertar detalle de ensayo a realizar]*** Ensayo 5: ***[insertar detalle de ensayo a realizar]***

Para superar esta fase, al menos ***[insertar]*** de las ***[insertar]*** unidades ensayadas no deberán presentar fallas y cumplir con la totalidad de la batería secuencial de ensayos físicos.

Los ensayos serán efectuados en presencia del comité de evaluación de las ofertas, bajo la veeduría técnica de ***[insertar nombre de entidad normativa]*** y observación de la ***[insertar nombre de entidad técnica]***.

Solamente las ofertas que superen estas Sub Fases pasarán a la siguiente

Fase, las ofertas que no la superen serán descalificadas.

11.4 FASE IV, Evaluación Económica

Se realizará la revisión aritmética de las ofertas presentadas y se harán las correcciones correspondientes.

Se compararán los precios totales de las ofertas evaluadas y se ordenarán de la más baja a la más alta evaluada.

IO-12 ERRORES U OMISIONES SUBSANABLE

Serán subsanables todos los errores u omisiones que no modifiquen la oferta en sus aspectos técnicos.

Solamente la subsanación de los errores aritméticos podrá afectar la oferta en sus aspectos Económicos de la siguiente forma:

- Diferencias entre las cantidades establecidas por el IHSS y las ofertadas, prevalecerán las cantidades establecidas por el IHSS.
- Inconsistencias entre precio mensual y precio total, prevalecerá el precio mensual

El valor de la oferta y el plazo de la Garantía de Mantenimiento de Oferta no serán subsanables.

IO-13 ADJUDICACION DEL CONTRATO

El contrato se adjudicará al ofertante que haya presentado la oferta con el precio más bajo y que cumpla sustancialmente con toda la documentación solicitada en estas bases de licitación.

El máximo porcentaje en que las cantidades podrán ser aumentadas es de acuerdo a demanda por incremento del servicio

El máximo porcentaje en que las cantidades podrán ser disminuidas es por reducción de necesidad del servicio.

Disposiciones Generales del Presupuesto 2018

ARTÍCULO 67.- En observancia a lo dispuesto en el Artículo 72, párrafos segundo y tercero, de la Ley de Contratación del Estado, la multa diaria aplicable se fija en cero puntos treinta seis por ciento (0.36%) por cada día de atraso en la disponibilidad en la prestación del servicio.

El valor de las multas a que se refieren los párrafos anteriores, estará en relación con el incumplimiento y el Monto de cada lote del contrato, estableciéndose éste cero puntos treinta seis por ciento (0.36%).

IO-14 FIRMA DE CONTRATO

El otorgamiento del contrato, se hará en un plazo máximo de ***10*** días hábiles, desde que la adjudicación quede en firme.

El oferente que resultare adjudicado deberá presentar de carácter obligatorio, previo a la firma del contrato, los siguientes documentos en un término de cinco (5) días hábiles contados a partir del día siguiente de su Notificación; lo anterior en cumplimiento a los artículos: 36 de la Ley de Contratación del Estado y 30 de su Reglamento:

a. Constancia de Solvencia Electrónica, extendida por el Servicio de Administración de Rentas (SAR) a excepción de empresas que tengan menos de un año de constituidas.
b. Original o copia de Constancia vigente de no haber sido objeto de resolución firme de cualquier contrato celebrado por la Administración extendida por la Procuraduría General de la República (PGR) a excepción de empresas que tengan menos de un año de constituidas.
c. Constancia del Instituto Hondureño de Seguridad Social (IHSS) de encontrarse al día en el pago de sus aportaciones o contribuciones., a excepción de empresas que tengan menos de un año de constituidas.
d. Certificación de Inscripción en el Registro de Proveedores y Contratistas de ONCAE.

De no presentar la documentación detallada en ese plazo, perderá todos los derechos adquiridos en la adjudicación y se procederá a adjudicar el contrato al ofertante que haya presentado la segunda oferta más baja evaluada y así sucesivamente.

SECCION II - CONDICIONES DE CONTRATACION

CC-01 ADMINISTRADOR DEL CONTRATO

El IHSS a través de la Gerencia de Tecnología de Información y Comunicación, será responsable de verificar la buena marcha y cumplimiento de las obligaciones contractuales, que entre sus funciones tendrá las siguientes:

a. Verificar que se emita la Orden de Inicio;
b. Dar seguimiento al cumplimiento en la prestación del Servicio;
c. Documentar cualquier incumplimiento del Contratista.

CC-02 PLAZO CONTRACTUAL

El contrato estará vigente desde su otorgamiento hasta doce (12) meses a partir de la firma-

CC-03 CESACIÓN DEL CONTRATO

El contrato cesará en sus efectos, por la expiración del plazo contractual o por el incumplimiento en la prestación del servicio.

CC-04 LUGAR DE ENTREGA DEL SUMINISTRO (PRESTACION DEL SERVICIO)

LOTE	Lugar de Entrega
LOTE 1: ADQUISICION DE EQUIPO DE COMUNICACIONES SWITCH CORE PARA EL CENTRO DE DATOS DEL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL	Gerencia de Tecnologias de Informacion y Comunicaciones, piso 8 del Edificio Administrativo del IHSS.
LOTE 2: EQUIPOS SWITCHES DE ACCESO PARA LA RED LAN DEL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL	Gerencia de Tecnologias de Informacion y Comunicaciones, piso 8 del Edificio Administrativo del IHSS.
LOTE 3: CERTIFICACION Y REPARACION DE CABLEADO DE FIBRA OPTICA (BACKBONE) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL	Gerencia de Tecnologias de Informacion y Comunicaciones, piso 8 del Edificio Administrativo del IHSS.
LOTE 4: SOLUCION DE FIREWALL DE SEGURIDAD PERIMETRAL DE PROXIMA GENERACION PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL	Gerencia de Tecnologias de Informacion y Comunicaciones, piso 8 del Edificio Administrativo del IHSS.

LOTE 5: ADQUISICION E INSTALACIÓN DE UNA SOLUCION DE COMUNICACIONES TELEFONICA IP DE CLASE EMPRESARIAL PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL	Gerencia de Tecnologías de Información y Comunicaciones, piso 8 del Edificio Administrativo del IHSS.

El lugar de entrega de los accesos (usuario y contraseña) y el link para la administración de la Prestación del Servicio es: Gerencia de Tecnologías de Información y Comunicación, 8 piso, Edificio Administrativo del IHSS, Barrio Abajo.

LOS OFERENTES DEBERÁN COTIZAR PRECIOS SEPARADOS POR LOTES

Esta licitación se adjudicará POR LOTES, por lo que se deberá presentar ofertas por UNO O VARIOS O EL TOTAL DE LOS LOTES.

CC-05 PLAZO Y CANTIDADES DE ENTREGA DEL SUMINISTRO

El plazo de entrega de los equipos y componentes será de conformidad como se describe a continuación:

LOTE 1: 60 días calendario para entrega y 30 para la instalación.
LOTE 2: 60 días calendario para entrega y 30 para la instalación.
LOTE 3: 60 días calendario la instalación.
LOTE 4: 60 días calendario para entrega y 30 para la instalación.
LOTE 5: 80 días calendario para entrega y 30 para la instalación.

Dicho tiempo se tomara en cuenta a partir de que la empresa reciba la Orden de Compra.

CC-06 PROCEDIMIENTO DE RECEPCION

Para la prestación del servicio y equipos, el contratista deberá coordinarse con el Almacén Central y con la Gerencia de Tecnología de Información y Comunicaciones, para programar el día y la hora para la recepción de los equipos por lotes según el lugar indicado.

CC-07 GARANTÍAS

Se aceptarán solamente fianzas y garantías bancarias emitidas por instituciones debidamente autorizadas, cheques certificados y bonos del Estado representativos de obligaciones de la deuda pública, que fueren emitidos de conformidad con la Ley de Crédito Público.

a) GARANTÍA DE CUMPLIMIENTO DE CONTRATO

- Plazo de presentación: diez (10) días hábiles posteriores a la firma del contrato.

- Valor: La garantía de cumplimiento del contrato deberá ser por el valor del quince por ciento (15%) de monto contractual para doce meses de la prestación del contrato.

- Vigencia: La garantía de cumplimiento del contrato deberá estar vigente hasta tres (3) meses posteriores a la fecha de vencimiento del contrato.

Esta garantía se incrementará en la misma proporción en que el valor del contrato llegase a aumentar.

b) GARANTIA DE BUEN SUMINISTRO

- Plazo de presentación: XX días hábiles después de la recepción final del suministro.
- Valor: La garantía de Calidad del contrato deberá ser por el valor equivalente al cinco por ciento (5%) de monto contractual, para los lotes 1,2, 4 y 5.
- Vigencia: el plazo ***de la vigencia de la garantía de calidad será de un año*** contado a partir de la recepción final por lote.

C) CERTIFICADO DE GARANTÍA DE FABRICACIÓN DEL SUMINISTRO: (No aplica)

- Plazo de presentación: ***[insertar número de días]*** días hábiles después de cada recepción parcial del suministro a satisfacción.
- Objeto: responder por reclamos por desperfectos de fábrica.
- Vigencia: [insertar el plazo de la vigencia de la garantía de buen suministro] contado a partir de la recepción final.

CC-08 FORMA DE PAGO

El pago del servicio se hará en forma única con informe de prestación de servicio o equipo conforme a lo estipulado en el contrato y aprobado por personal contraparte designado por la Gerencia de Tecnología de Información y Comunicación, será pagada por el INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL y sin recargo alguno, dicho pago y se efectuará en moneda de curso legal en Honduras (Lempira). Para el pago se debe presentar un informe del servicio y una factura o recibo.

El Instituto Hondureño de Seguridad Social**,** a través de la Gerencia Administrativa y Financiera, efectuará los trámites de pago conforme a los procedimientos establecidos por el INSTITUTO.

LOTE	DESCRIPCION	FORMA DE PAGO
1	**ADQUISICION DE EQUIPO DE COMUNICACIONES SWITCH CORE PARA EL CENTRO DE DATOS DEL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL**	
	Equipo de comunicaciones integrado que incluye:	
	a) Componente de comunicaciones modular de clase empresarial tipo switch CORE	Pago único conforme a

		Entrega
	b) Componente de seguridad interna (NGFW).	Pago único conforme a Entrega
	c) Componente de administración y monitoreo	Pago único conforme a Entrega
	Servicio de Instalación, configuración, pruebas, verificación del correcto funcionamiento de la solución de infraestructura, equipos, componentes y su software de gestión, incluyendo los accesorios, patchcords, medios, equipos, software, etc que sean necesarios para la instalación y puesta en producción del equipo.	Pago único conforme a Entrega
	Servicio de Capacitación por parte del representante del fabricante en el uso, administración, configuración y monitoreo de la solución adquirida para el Área de Infraestructura de la Gerencia de IT del IHSS, para ocho personas un mínimo	Pago único conforme a Entrega
	Servicio de Soporte Técnico por un año para toda la solución	
	Servicios de Suscripción con el fabricante por un año: el equipo deberá contar con una suscripción para descarga de archivos de definiciones de manera automática para todos los componentes de la solución, la cual deberá incluir soporte técnico (local y remoto cuando fuera necesario), actualizaciones y corrección de errores	Cinco días después de firma del contrato por suscripción.
	TOTAL LOTE 1 (Componentes, Servicios y Accesorios)	
2	**EQUIPOS SWITCHES DE ACCESO PARA LA RED LAN DEL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL**	
	Equipos	Pago único conforme a Entrega
	Servicios de instalación y configuración	Pago único conforme a Entrega
	Servicio de Soporte Técnico por un año	Pago único conforme a Entrega
	TOTAL LOTE 2 (Componentes, Servicios y Accesorios)	
3	**CERTIFICACION Y REPARACION DE CABLEADO DE FIBRA OPTICA (BACKBONE) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL**	
	Suministro de patchcords de fibra óptica	Pago único conforme a Entrega
	Diagnóstico de los enlaces de fibra óptica que incluya la validación de capacidades de cada línea y la limpieza de gabinetes, conectores y adaptadores actualmente instalados.	Pago único conforme a Entrega
	Servicio de Reparación de fibra óptica	Pago único conforme a

		Entrega
	Servicio de Certificación de fibra óptica	Pago único conforme a Entrega
	TOTAL LOTE 3 (Insumos, Servicios y Accesorios)	
4	**SOLUCION DE FIREWALL DE SEGURIDAD PERIMETRAL DE PROXIMA GENERACION PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL**	
	Equipo de seguridad perimetral integrado que incluye:	
	a) Componente de seguridad perimetral	Pago único conforme a Entrega
	b) Componente de Administración y monitoreo	
	Servicio de Instalación, configuración, pruebas, verificación del correcto funcionamiento de la solución de infraestructura, equipos, componentes y su software de gestión, incluyendo los accesorios, medios, equipos, etc que sean necesarios para la instalación y puesta en producción del equipo.	Pago único conforme a Entrega
	Servicio de Capacitación por parte del representante del fabricante en el uso, administración, configuración y monitoreo de la solución adquirida para el Área de Infraestructura de la Gerencia de IT del IHSS, para seis personas un mínimo.	Pago único conforme a Entrega
	Servicios de Suscripción con el fabricante por un año: el equipo deberá contar con una suscripción para descarga de archivos de definiciones de manera automática para todos los componentes de la solución, la cual deberá incluir soporte técnico (local y remoto cuando fuera necesario), actualizaciones y corrección de errores.	Cinco días después de firma del contrato por suscripción.
	TOTAL LOTE 4 (Componentes, Servicios y Accesorios)	
5	**ADQUISICION E INSTALACIÓN DE UNA SOLUCION DE COMUNICACIONES TELEFONICA IP DE CLASE EMPRESARIAL PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL**	
	3 equipos de comunicación telefónica IP, que incluye:	
	a) Componente de Comunicaciones de Telefonía IP	Pago único conforme a Entrega
	b) Componente de administración y monitoreo	Pago único conforme a Entrega
	Servicio de Instalación, configuración, pruebas, verificación del correcto funcionamiento de la solución de infraestructura, equipos, componentes y su software de gestión; incluyendo todos los accesorios, medios, equipos, etc que sean necesarios para la puesta en producción del equipo.	Pago único conforme a Entrega

	Servicio de Capacitación por parte del representante del fabricante o representante en el uso, administración, configuración y monitoreo de la solución adquirida para el Área de Infraestructura de la Gerencia de IT del IHSS, para ocho personas un mínimo.	Pago único conforme a Entrega
	Servicio de Soporte técnico (local y remoto cuando fuera necesario), actualizaciones y corrección de errores.	Pago único conforme a Entrega
	TOTAL LOTE 5 (Componentes, Servicios y Accesorios)	
	GRAN TOTAL	

CC-09 MULTAS

Cuando el contratista incumpla las obligaciones establecidas en el contrato, por causas imputables al mismo, se le impondrá el pago de una multa del 0.36% del monto del servicio por cada día de atraso en la disponibilidad solicitada, sin perjuicio de las obligaciones pactadas. Si la demora no justificada diera lugar a que el total cobrado por la multa aquí establecida ascendiera al diez por ciento (10%) del valor parcial del contrato "EL INSTITUTO", podrá considerar la resolución total del contrato y hacer efectiva la garantía de cumplimiento, sin incurrir por esto en ninguna responsabilidad de su parte.

SECCION III - ESPECIFICACIONES TECNICAS

ET-01 NORMATIVA APLICABLE (NO APLICA)

ET-02 CARACTERÍSTICAS TECNICAS
Todo esto es la oferta técnica

a) Descripción de la solución.
b) Especificaciones Técnicas ofertadas.
c) Esquema de soporte técnico en caso de fallas, incluyendo procedimiento de escalamiento de casos.
d) Descripción del servicio de soporte técnico y mantenimiento.
e) Hojas de vida del personal técnico.
f) Lista de personal técnico.
g) Material informativo del oferente que explique los aspectos técnicos y operativos incorporados en su propuesta.
h) Constancia de que el personal a cargo de la instalación, mantenimiento y soporte técnico del servicio tiene la experiencia de los dos (2) últimos años en proyectos similares desempeñados. Presentando Hoja de Vida y al menos dos (2) Constancias de los últimos dos años en proyectos similares, además debe de adjuntar los datos teléfono, dirección y persona contacto.
i) Declaración jurada debidamente autenticada expresando: Experiencia que el oferente tiene con los servicios y productos que ofrece; detalle de cuántas plataformas similares a las que ofrece ha implementado con éxito anteriormente,

LOTE 1: ADQUISICION DE EQUIPO DE COMUNICACIONES SWITCH CORE PARA EL CENTRO DE DATOS DEL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

El IHSS requiere de la adquisición de una solución de comunicaciones integral de clase empresarial, robusta, modular, escalable, comprendida por un equipo de Comunicaciones CORE, un módulo firewall de próxima generación para seguridad de la red interna, módulo de administración y monitoreo para ser utilizada en su Centro de datos principal en Tegucigalpa.

La propuesta debe incluir el equipo con lo siguiente:

- Componente de comunicaciones modular de clase empresarial tipo switch CORE.
- Componente de seguridad interna (NGFW).
- Componente de administración y monitoreo (dispositivo, softwares y servicios).
- Instalación, configuración, pruebas, verificación del correcto funcionamiento de la solución de infraestructura, equipos, componentes y su software de gestión.
- Capacitación por parte del representante del fabricante en el uso, administración, configuración y monitoreo de la solución adquirida para el Área de Infraestructura de la Gerencia de IT del IHSS, para seis personas un mínimo.
- Servicio de Soporte Técnico por un año.
- Servicio de garantía del fabricante: los equipos, todos sus componentes de hardware y software deben de tener una garantía 1 año como mínimo.
- Servicios de Suscripción con el fabricante por un año: el equipo deberá contar con una suscripción para descarga de archivos de definiciones de manera automática para todos los componentes de la solución, la cual deberá incluir soporte técnico (local y remoto cuando fuera necesario), actualizaciones y corrección de errores.

- El proveedor deberá incluir todos los accesorios, patchcords, medios, equipos, software, etc que sean necesarios para la puesta en producción del equipo.

GENERALES:

El proveedor deberá suministrar, instalar, configurar y poner en operación la solución de telecomunicaciones en base a la configuración propuesta por el IHSS; las actividades que deberán estar incluidas son:

- Montar y fijar los equipos de telecomunicaciones en los racks o gabinetes;
- Energizar los equipos;
- Realizar la desconexión de patchcords de los equipos actuales y conectarlos a los equipos que se suministre.
- Realizar la migración o configuración a los nuevos equipos a suministrar.
- Validar pruebas de conexión en conjunto con personal del área de Infraestructura de la Gerencia de Tecnologías de Información y Comunicaciones.

DESCRIPCIÓN DEL SERVICIO:

1. Durante la vigencia del contrato de soporte el proveedor deberá colaborar en realizar las configuraciones necesarias por el IHSS en los equipos provistos en conjunto con el Área de Infraestructura de la Gerencia de Tecnologías de Información y Comunicaciones.
2. Apoyará al IHSS para la buena operación de los equipos de telecomunicaciones y deberá reemplazar los equipos o componentes que sean necesarias durante la vigencia de la garantía.
3. Se proporcionará soporte técnico telefónico, remoto o en sitio cuando los incidentes presentados así lo ameriten.
4. Proporcionará un número telefónico directo y correo electrónico para recibir las solicitudes de soporte técnico.
5. Deberá atender y solucionar cualquier incidente reportado, atendiendo en un máximo de 2 horas y resolviendo según el caso en un máximo de 24 horas, sustitución del equipo o brindando alguna alternativa de solución.
6. Entregar una matriz de escalamiento de problemas con nombres, teléfonos fijo o celular y direcciones de correo electrónico.
7. La infraestructura de red del IHSS está basada protocolos estándares de la industria, por lo que las configuraciones deberán de poderse integrar a la infraestructura existente e instalada sin deteriorar los servicios de comunicaciones.
8. La empresa deberá entregar nota del fabricante de la solución donde se indique que esta cuenta con la capacidad técnica y el respaldo de la marca y del fabricante para el tipo de implementación de productos y servicios descritos en el LOTE 1: ADQUISICION DE EQUIPO DE COMUNICACIONES SWITCH CORE PARA EL CENTRO DE DATOS DEL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL.

CARACTERISTICAS DE LOS EQUIPOS DE COMUNICACIÓN

ESPECIFICACIONES GENERALES DE LA SOLUCION	
Garantía del fabricante	Todos los equipos y sus componentes de hardware y software deben de tener una garantía 1 año como mínimo.
Soporte	Los equipos deberán contar con soporte técnico local o remoto en los casos que amerite durante un año. Este contrato debe incluir la configuración inicial y puesta en producción del equipo en el sitio, resolución de fallos y requerimientos adicionales en las configuraciones. Deberá ser brindado por un representante local del fabricante.
Accesorios	Para todos los puertos deberán incluirse los patchcords de fibra óptica de 3 metros de longitud (después de adjudicado se hará revisión de los tipos de conectores a usar). Así mismo se deberá incluir: • Los accesorios necesarios para la realización de instalación de equipos. • Los cables de conexión eléctrica AC • La totalidad de los Módulos de fibra óptica en sus interfaces • Documentación del equipo en físico o electrónico. • Patchcords de conectividad Ethernet de 5 metros de longitud.
Capacitación	Se deberá brindar capacitación técnica en el uso de la totalidad de la solución de comunicaciones, incluyendo sus diferentes módulos o componentes. Deberá ser otorgada por un representante del fabricante de manera presencial, con una duración estimada de al menos 40 horas y para al menos 8 personas de la Gerencia de IT del IHSS.
Servicios de Suscripción	Servicios de Suscripción con el fabricante por un año: el equipo deberá contar con una suscripción para descarga de archivos de definiciones de manera automática para todos los componentes de la solución, la cual deberá incluir soporte técnico (local y remoto cuando fuera necesario), actualizaciones y corrección de errores.
Visitas de Campo	En la visita de campo a las instalaciones del IHSS en Tegucigalpa, el oferente podrá

	verificar y validar la compatibilidad de la infraestructura de comunicaciones del IHSS con la solución ofertada.

ESPECIFICACIONES TECNICAS MINIMAS						
SWITCH CORE MODULAR DE CLASE EMPRESARIAL						
1. Especificaciones General			**Cumple**		**Folio**	**Observación**
			Si	**No**		
	1. Descripción	Solución de comunicaciones de clase empresarial, robusta, modular, comprendida por un equipo de Comunicaciones CORE y un módulo firewall de próxima generación (NGFW) de seguridad interna				
	2. Cantidad	1				
	3. Arquitectura	El equipo deberá ser de arquitectura tipo Chasis modular, con al menos 07 slots o ranuras para tarjetas de línea y tarjetas supervisoras.				
	4. Redundancia en tarjetas supervisoras	El equipo deberá tener redundancia N+1 para tarjetas supervisoras.				
	5. Redundancia en ventiladoras	El equipo deberá tener redundancia N+1 para ventiladores.				
	6. Redundancia en fuentes de poder	El equipo deberá tener, al menos, 2 fuentes de poder. Estas fuentes deben poder ser reemplazadas en caliente.				
	7. Tecnologías	El equipo deberá debe contar con, al menos, las tecnologías de siguiente generación que se listan a continuación: • Asignación configurable basada en plantillas de: forwarding en capas 2 y 3, ACLs (Access Control Lists) y QoS (Quality of Service).				
	8. Procesamiento y	El equipo deberá tener al				

	memoria	menos una CPU x86 con 16 (diez y seis) GB de memoria RAM y 10 GB de memoria Flash o SSD. La memoria flash o SSD especificada debe estar embebida en el equipo.				
	9. Aislamiento Sistema Operativo	El equipo deberá asegurar máxima flexibilidad y aislamiento del sistema operativo principal.				
	10. Puerto USB	El equipo deberá contar con un puerto USB como opción para cargar el sistema operativo y configuraciones.				
	11. Ejecución de scripts python	El equipo deberá soportar la ejecución de scripts usando Python directamente desde el switch (on-box Python). De esta manera los scripts de Phyton pueden aprovechar la conexión directa con el dispositivo.				
	12. Tarjetas con SFP+	El equipo deberá contar con, al menos, 2 tarjetas con 24 puertos basados en SFP+ cada una.				
	13. Tarjeta con RJ45	El equipo deberá contar con una tarjeta con 48 puertos basados en RJ45, con velocidad de 10/100/1000 Mbps, compatible con PoE y PoE+, preparado para IEEE 1588/802.1as, Ethernet de eficiencia energética (EEE).				
	14. Ancho de banda por slot	El chassis del switch deberá proporcionar un ancho de banda por slot de 450 Gbps				
	15. Rendimiento	El switch deberá ofrecer, al menos, el siguiente rendimiento: • Capacidad de conmutación: 120 Gbps por slot. • Capacidad de transmisión: 900 Mbps				
	16. VLANs	El equipo deberá poder manejar, al menos, 4000 identificadores de VLANs				

	17. Jumbo Frames	El equipo deberá poder manejar jumbo frames con un tamaño mínimo de 9000 bytes.				
	18. Mecanismos QoS	El equipo deberá contar con, al menos, los siguientes mecanismos de QoS: • 802.1p CoS (Class of Service). • Clasificación DSCP (Differentiated Services Code Point). • Planificación SRR (Shaped Round Robin). • CIR (Committed Information Rate). • Class Based weighted fair queuing (CBWFQ) • QoS Jerárquico (H-QoS) • Weighted Random Early Detection (WRED) • Manejo de prioridad a nivel de colas, ocho colas de salida por puerto basado en hardware. • Marcado y clasificación de paquetes basado en dirección IP origen y destino, MAC origen y destino y numero de puertos TCP y UDP. • Configuración automática de QoS				
	19. Protocolos Estándar	El equipo deberá poder enrutar el tráfico mediante cualquiera de los siguientes protocolos estándar: • OSPF • BGP • Policy based routing • PIM • VRRP (Virtual router redundancy protocol) • IP SLA (service level agreement) • VRF				
	20. API REST	El equipo deberá soportar APIs				

		REST que puedan interactuar directamente con el sistema operativo del switch				
	21. Soportar Spanning Tree	El equipo deberá soportar Spanning Tree IEEE 802.1d así como las mejoras tales como convergencia rápida (RSTP 802.1w) y múltiples instancias (MSTP 802.1s).				
	22. Operación de puertos	Los equipo del switch deberán poder operar en half y full dúplex.				
	23. Soporte NTP e IGMP	El equipo deberá soportar NTP e IGMP.				
	24. Agregación de puertos	El equipo deberá soportar Agregación de puertos, LACP, IEEE 802.3ad, de modo que se pueda usar cualquier puerto del mismo tipo y velocidad.				
	25. Puertos de administración	El equipo deberá contar con los siguientes puertos para administración: • Puerto de consola: RJ45 • Puerto ethernet dedicado para administración fuera de banda.				
	26. Soporte SYSLOG	El equipo deberá soportar syslog				
	27. Administración WEB	El equipo debe soportar administración vía web.				
	28. Niveles de acceso	El equipo deberá soportar múltiples niveles de privilegios de acceso (mínimo 4) por puerto de consola o Telnet para administración.				
	29. Filtros de acceso	Para asegurar una óptima seguridad en la gestión, el equipo deberá soportar la configuración de filtros de acceso que sólo permitan el acceso a determinadas IP en los puertos de gestión.				
	30. Soporte DEBUG	El equipo deberá soportar procesos de debug para análisis en caso de fallas				
	31. Limitar direcciones MAC	El switch deberá tener la capacidad de limitar la				

		cantidad de direcciones MAC aprendidas en un puerto para evitar ataques MAC address flooding que llenen la tabla de direcciones MAC del switch.				
	32. Mecanismos de prevención de ataques	El switch deberá soportar mecanismos para evitar ataques tipo MITM, basados en STP y DHCP, así como "VLAN Hopping", "DHCP Rogue Server".				
	33. Filtros aplicables por puertos	El switch deberá soportar filtros aplicables por puerto, filtros basados en direcciones MAC de origen y destino, direcciones IP de origen y destino y puertos TCP/UDP				
	34. Autenticación con asignación dinámica	El switch deberá soportar de autenticación 802.1x con asignación dinámica de VLAN y asignación dinámica de listas de control de acceso (ACL).				
	35. Control de acceso centralizado	El switch deberá soportar control de acceso centralizado por RADIUS, ya sea para los administradores del switch como para los usuarios de la red que se autentican vía 802.1x.				
	36. Soporte a movilidad MAC	El switch deberá soportar movilidad de MAC en esquemas de 802.1x detrás de un teléfono, permitiendo que al ser autenticado el usuario conectado a un teléfono y luego de su desconexión, el switch pueda recibir información de la desconexión a pesar de no estar usuario físicamente conectado al switch, evitando el spoofing de la MAC.				
	37. Autenticación por MAC	El switch deberá soportar 802.1x, autenticación por MAC (MAB) y Web Authentication de manera dinámica para usuarios que se conectan detrás de un teléfono IP				

	38. Análisis de trafico	El switch deberá soportar análisis de tráfico usando protocolos tipo Netflow o similares. El análisis de tráfico debe de ser tanto en el downlink como en el uplink.				
	39. Port Mirroring	El switch deberá soportar "port mirroring" por puerto y por VLAN.				
	40. Sesiones Port Mirroring	El switch deberá soportar múltiples sesiones de "port mirroring" así como "port mirroring" remoto.				
	41. Firma criptográfica en software	El software del switch deberá estar firmado criptográficamente; cuando el equipo inicia, las firmas del sistema operativo son verificadas. Se deberá ofrecer información pública con los procedimientos para garantizar la autenticidad del software				
	42. Soporte boot seguro	El switch deberá soportar boot seguro a prueba de manipulaciones, para asegurar que solamente el sistema operativo del fabricante pueda ser ejecutado en el hardware del mismo haciendo verificaciones procesador, memoria y ROM de arranque.				
2.	**Escalabilidad**					
	1. Memoria de Buffer	El switch deberá tener una memoria buffer para paquetes de, al menos, 16 (dieciséis) MB.				
	2. Transmision de paquetes	El switch deberá debe soportar transmisión de paquetes IPv6 en hardware.				
	3. Soporte Dual-Stack	El switch deberá debe soportar dual-stack IPv4/IPv6 para facilitar la migración de IPv4 a IPv6.				
	4. Escalabilidad	El equipo deberá tener posibilidad de crecer en puertos de 1Gbps, 10Gbps y 40 Gbps ya sea a través de				

		puertos embebidos o tarjetas modulares adicionales.				
3. Seguridad						
	1. Soporte MACSEC	El equipo deberá debe soportar cifrado MACSEC (802.1AE) en todos los puertos y a todas las velocidades.				
	2. Análisis de información de eventos	Se debe incluir una solución que permita el uso de algoritmos avanzados de análisis de comportamiento; para identificar patrones de tráfico, usando análisis de la información de eventos que ocurren dentro de un flujo de datos aplicando técnicas de machine learning, con el objetivo de detectar potenciales amenazas de seguridad. Esto deberá hacerse con tecnologías propias de la solución propuesta; o a través de la inclusión de hardware y software adicional que permita descifrar el tráfico para su análisis				
	3. Detección de malware	La precisión a la hora de detectar malware en tráfico cifrado HTTPS debe ser de, al menos, el 99 (noventa y nueve) %.				
	4. Falso positivo	Los falsos positivos a la hora de detectar malware en tráfico cifrado HTTPS debe ser, como mucho, del 1 (uno)%.				
	5. Identificación de mecanismos de encriptación	La solución deberá debe permitir identificar los distintos mecanismos de encriptación que se están usando en la red.				
	6. Detección de ataques	La solución deberá permitir detectar: ataques de denegación de servicio (DoS) y de denegación de servicio distribuido (DDoS) incluyendo inundaciones de todo tipo (ICMP, UDP, TCP SYN, TCP				

		NULL, IP NULL, etc), presencia de botnets en la red, suplantación DNS, exploits de día cero, malware auto modificador, ataques en el tráfico cifrado o mal uso de recursos o configuración incorrecta de los dispositivos de comunicación (como por ejemplo errores de configuración en la segmentación de las VLANs).				
	7. Detección de anomalías	En caso de usar IPFIX, Netflow o protocolos similares para realizar la detección de anomalías de seguridad descrita en esta sección, los switches deben tener la capacidad de generar de forma conjunta como mínimo 200 (doscientos) flujos por segundo mediante la utilización de protocolos Netflow o similares. Estos flujos deberán ser usados para detectar anomalías en el tráfico.				
4. Automatización						
	1. Software de interfaz grafica	El equipo deberá soportar la automatización de las siguientes funciones, mediante el uso de un software con interfaz gráfica, el cual se debe incluir en la solución: • El switch debe poder ser dado de alta automáticamente. Esto es aprovisionamiento "zero-touch" • Plantillas de configuración • Obtención de información de inventario de los equipos • Administración de versiones de software: estandarización de imágenes de software,				

		verificaciones antes y después de realizar el despliegue de nuevas versiones de software en los switches. • Generación de grupos de dispositivos para simplificar tareas administrativas • Despliegue de políticas de Calidad de Servicio (QoS) • Políticas de control de acceso • Segmentación automatizada basada en políticas de usuarios, dispositivos y etc, usando un overlay o fabric de red automatizado. La segmentación de usuarios debe poder hacerse en base a sus respectivos roles en la institución. La configuración de estas políticas debe poder hacerse en un entorno gráfico, de manera centralizada y debe estar preparado para tener una misma política en redes cableadas e inalámbricas.				
5. Monitoreo y Aseguramiento de Servicios						
	1. Software de Monitoreo	La solución deberá soportar la automatización de las siguientes funciones, mediante el uso de un software con interfaz gráfica, el cual se debe incluir en la solución: • Analíticos de la salud general de los dispositivos de infraestructura de red. • Analíticos de conectividad de los dispositivos finales conectándose a la red, mediante la recolección de información con respecto a DHCP, estado				

		de los puertos, autenticación, etc • Funcionalidad de búsqueda de dispositivos de infraestructura de red y usuarios.				
6. Requerimientos de operación						
	1. Temperatura de entorno físico	La solución deberá poder operar en un entorno físico cuya temperatura oscile entre los 0 y los 40 grados centígrados.				
	2. Humedad relativa en entorno	La solución deberá poder operar en un entorno físico cuya humedad relativa esté entre el 10 y el 90 por ciento.				
	3. MTBF	La solución deberá tener al menos, un MTBF de 300,000 horas para la tarjeta supervisora del sistema y al menos un MTBF de 270,000 horas para las tarjetas ó modulos.				
7. Control de Acceso						
	1. Software de control de acceso de red	La solución deberá incluir un software de control de acceso de red que soporte las siguientes funcionalidades para al menos 200 dispositivos: • Perfilar (identificar) el tipo de dispositivo que se conecta a la red. • Poder registrar dispositivos personales en la red de SEDAPAL (BYOD) • Autenticación, autorización y registro (AAA) • Administración de cuentas de invitado				
8. Soporte						
	1. Servicio de Suscripción	La solución deberá contar con una suscripción por, al menos de 1 año que incluya lo siguiente: • Soporte y acceso a las				

		actualizaciones del software de la solución la validez de la suscripción. • Apertura de casos y posibilidad de acceso directo con el fabricante para la resolución de problemas.				
9. Garantías						
	1. Equipo nuevo	Toda la solución debe ser nueva, no re manufacturados y garantizados contra defectos de fabricación.				
	2. Garantía avalada por el fabricante	La solución deberá contar con soporte técnico avalado por el fabricante durante 1 año.				
	3. Beneficios de la garantía	El soporte avalado por el fabricante debe brindar los siguientes beneficios durante su vigencia: • Reemplazo del equipo y/o sus partes bajo modalidad 8x5xNBD (8 horas laborables al día, 5 días laborables de la semana y reemplazo en sitio al siguiente día laborable una vez que el fabricante ha confirmado el daño del equipo y/o sus partes). • Acceso a actualizaciones del sistema operativo y parches de seguridad, etc. • Apertura de casos con un representante del fabricante de la solución para la resolución de problemas.				
MODULO FIREWALL DE PROXIMA GENERACION DE CLASE EMPRESARIAL						
1. Especificaciones General						
	1. Descripción	Solución de firewall de próxima generación (NGFW) integrado y centralizado en amenazas con administración unificada, para protección de la red interna del IHSS, al menos con los siguientes				

		módulos: • Control de Aplicaciones • Sistema de Protección y Detección de Intrusos de Siguiente Generación (Next Generation IPS, NGIPS) • Conciencia Contextual y Automatización de Seguridad • Inteligencia de Seguridad • Detección y remediación avanzada de Malware • Filtrado URL • Plataforma de Gestión				
	2. Cantidad	1				
	3. Integrado a la plataforma de la solución de comunicaciones	Debe estar basado en una plataforma de hardware (appliance) de propósito específico. El hardware y software de la solución propuesta deben ser del mismo fabricante. No se deberán proponer appliance tales como routers ni servidores cuya función secundaria sea IPS.				
	4. Rendimiento (FW + Control de Aplicaciones)	Rendimiento de 8.5 Gbps en modalidad FW + Control de Aplicaciones				
	5. Rendimiento (FW + Control de Aplicaciones + NGIPS)	Rendimiento de 8.5 Gbps con funcionalidades de firewall + Control de Aplicaciones + NGIPS				
	6. Sesiones concurrentes (Control de Aplicaciones)	Soportar un mínimo de 3 millones de sesiones concurrentes con control de Aplicaciones				
	7. Nuevas conexiones concurrentes (control de aplicaciones)	Soportar un mínimo de 40,000 nuevas conexiones concurrentes, con Visibilidad y Control de aplicaciones.				
2. Características Básicas						
	1. Modo de despliegue	Despliegue simultáneo en modo transparente y / o enrutador.				
	2. Compatibilidad	Compatibilidad con OSPF y				

	OSPF	BGP (v4 y v6).				
	3. Tipos de NAT	NAT dinámico y estático.				
	4. Capacidad de configuración	Debe poder soportar capacidad de configuración de recuperación de falla / configuración de alta disponibilidad. (Posibilidad para adicionar y configurar a futuro otro equipo físico).				
	5. Inspección de paquetes	Protocolo de inspección de todos los paquetes en todos los flujos.				
	6. Soporte VPN	Soporte integrado VPN de sitio a sitio y de acceso remoto.				
	7. Software Defined Network	Integración con Redes Definidas por Software (*Software Defined Networks*, SDN).				
	8. QoS	QOS y limitación de velocidad.				
	9. Implementaciones de puerta de enlace	Las implementaciones de puerta de enlace deben admitir L2 (transparente) y L3 con topologías de alta disponibilidad. Las transiciones de HA deben ocurrir sin problemas con o sin STP y reaccionar o ignorar el estado de enlace físico.				
	10. Compatibilidad con IPv6	La compatibilidad con IPv6 debe incluir tecnologías de próxima generación como IPS, Control de aplicaciones, Filtrado de URL y Anti-Malware.				
	11. Soporte a diferentes integraciones	Soporte a integración con switches vía Multi-Chassis Ether Channel, combinado con balanceo por medio de ruteo ECMP (Equal-Cost MultiPath)				
	12. Soporte a protocolos	Capacidad de soportar OSPF, IETF, Non-Stop Forwarding, OSPF Fast-Hello y BGP Graceful Restart.				
3. Control de Aplicaciones						
	1. Soporte a aplicaciones	Soporte a más de 4,000 aplicaciones				
	2. Soporte a	Soporte a geolocalización -				

	geolocalización	permitiendo obtener al menos la siguiente información: país, longitud, latitud, zona horaria.				
	3. Soporte a OpenAppID	Soporte a OpenAppID				
	4. Rendimiento con control de aplicaciones	Mantiene el rendimiento mientras realiza el control de aplicaciones				
	5. Gama de aplicaciones	Capacidad para reconocer y controlar una amplia gama de aplicaciones.				
	6. Creación de identificadores de aplicaciones	Capacidad de permitir a los administradores la creación de identificadores de aplicación e importar identificadores de aplicación previamente construidos por comunidades de open source.				
	7. Relevancia de aplicación	La identificación de la aplicación incluye la relevancia y el riesgo del negocio.				
	8. Lenguajes de código abierto	Detección de aplicaciones personalizadas a través de un lenguaje de firma abierto.				
	9. Nivel de riesgo de aplicaciones	Capacidad para controlar aplicaciones por nivel de riesgo / relevancia del negocio.				
	10. Agrupación de aplicaciones	Capacidad para controlar aplicaciones por usuario o grupo.				
	11. Control de sub-aplicaciones	Capacidad para controlar sub-aplicaciones o funcionalidad de aplicación específica.				
4. Sistema de Protección y Detección de Intrusos de Siguiente Generación (Next Generation IPS, NGIPS)						
	1. Soporte a modo transparente	El dispositivo podrá configurarse en modo transparente; es decir de detección en línea, pero sin bloquear tráfico. El sistema solo alerta que eventos fueron bloqueados.				
	2. Monitoreo en modo transparente	Cuando en modo transparente, el monitoreo del dispositivo debe ser transparente para los usuarios				

		y operar en la capa 2 del modelo de OSI, por lo que las interfaces no requieren de una dirección de IP ni una MAC.				
	3. Puntualización de tráfico en modo transparente	El dispositivo debe permitir la configuración de modo transparente para todo el tráfico o apenas para paquetes especificados por dirección IP, protocolo, VLAN ID incluyendo frames 802.1q				
	4. Detección de trafico anómalo	El dispositivo debe tener la capacidad de detectar trafico anómalo o vulnerabilidades en las siguientes aplicaciones IM y P2P: AOL Instant Messeger; MSM Messenger; Yahoo! Messenger; ICQ; Gnutella; Kazza; eDonkey; BitTorrent; SoulSeek.				
	5. Inspección de tráfico por diferentes segmentos de red	El dispositivo debe ser capaz de inspeccionar el trafico asociado a distintos segmentos de redes diferentes (en lugar de tener una sola política por interfaz)				
	6. Edición de reglas pre - configuradas	Posibilidad de editar las reglas existentes.				
	7. Creación de reglas personalizadas	Capacidad para crear reglas personalizadas utilizando el motor nativo				
	8. Creación de reglas basadas en varios elementos	Capacidad de crear reglas de control basadas en zonas, subredes, aplicaciones, usuarios, puertos, categorías de URL y su reputación, así como asociar su política de prevención de intrusos y análisis de malware correspondiente. Todo esto deberá poder ser configurado en una sola regla de acceso.				
	9. Prever la detección de anomalías	Debe prever la detección de anomalías de tráfico y análisis de impacto por evento para evitar ataques de día cero, como una funcionalidad dentro del mismo dispositivo y				

		sin necesidad del uso de aplicaciones adicionales como sistema de detección de anomalías o scanners				
	10. Generación de datos de flujo de red	Capacidad para generar datos de flujo de red (Netflow)				
	11. Evaluacion de impacto	Evaluación de impacto automatizada basada en datos de perfiles y vulnerabilidades de host.				
	12. Listados basados en feeds	IP y listas negras de URL y listas blancas basadas en feeds incorporados o personalizados y listas.				
	13. DNS sink-holing	DNS sink-holing basado o construido en feeds personalizados y listas.				
	14. Protección contra spyware	El dispositivo debe poder contar con protección contra spyware				
	15. Basado en firmas de vulnerabilidades	El dispositivo debe estar basado sobre firmas de vulnerabilidades permitiendo la detección de ataques desconocidos o variaciones de ataques conocidos.				
	16. Recomendación de afinamiento	Deberá ser capaz de hacer recomendación de afinamiento de políticas en base a la información aprendida de la red, mostrando un registro de las reglas recomendadas. La función de recomendación de afinación de políticas es opcional.				
	17. Identificación de vulnerabilidades en host	Deberá identificar vulnerabilidades de los host de la red en tiempo real y sin necesidad de correr un análisis de vulnerabilidades.				
	18. Capacidad para catalogar dispositivos	Capacidad de descubrir, perfilar y catalogar los hosts, sistemas operativos y sus versiones, vulnerabilidades, aplicaciones servidores y cliente que existen dentro de				

		la red del convocante, y que la política de IPS provea recomendaciones para proteger estos dispositivos al administrador y se adapte automáticamente a los cambios dentro del entorno.				
	19. Capacidad de análisis dinámico	Capacidad de hacer análisis dinámico (sandboxing) y aprendizaje máquina para detección de ataques avanzados.				
5. Conciencia Contextual y Automatización de Seguridad						
	1. Solución adaptativa	NGIPS/NGFW adaptativo en tiempo real (basado en la evaluación dinámica de la red - automáticamente deberá saber que pasa en la red).				
	2. Automatización de tareas	Capacidad para automatizar completamente tareas como informes, actualizaciones, copias de seguridad, etc.				
	3. Priorización automática de eventos	Priorización automática de eventos de amenazas basados en la relevancia para el medio ambiente protegido.				
	4. Soporte a indicadores de compromiso	Soporte a Indicadores de Compromiso (IoC) basados en la relevancia para el medio ambiente protegido.				
	5. Ajuste automático política de intrusión	Capacidad para ajustar automáticamente la política de intrusión basada en dispositivos en un entorno protegido.				
	6. Configuración de lista blanca	Lista blanca de diversos conjuntos de dispositivos (impresoras, routers, etc) / sistemas operativos / aplicaciones / servicios.				
	7. Soporte con protocolos varios	El dispositivo debe mostrar qué usuario está generando o recibiendo el evento detectado apoyándose de los siguientes protocolos: LDAP, POP3, SIP, IMAP, AIM (sin necesidad de hardware o software separado).				

	8. Integración activa	Integración activa con soluciones de control de acceso para remediación automatizada y respuesta.				
	9. Soporte integrado para etiquetado	Soporte totalmente integrado para el etiquetado de grupos de seguridad para permitir la seguridad basada en políticas, independiente de la topología.				
6. Inteligencia de Seguridad						
	1. Colección de inteligencia	Colección de inteligencia de amenazas: • Correo electrónico: 200 mil millones de correos electrónicos maliciosos al día, o 2,3 millones de bloques por segundo • Visibilidad web: Análisis sobre casi 17 mil millones de solicitudes web cada día • Real-time malware análisis: Más de 1.100.000 muestras de software malicioso al día				
	2. Soporte a fuentes de terceros	Soporte a fuentes de inteligencia de terceros con soporte a STIX y TAXII				
	3. Formatos abiertos	Contenido entregado en formatos abiertos para permitir la polinización cruzada de herramientas de seguridad.				
	4. Análisis de profundidad	Análisis en profundidad realizado por la organización de investigación.				
	5. Aplicación a toda la solución	Enfoque de la inteligencia de amenazas, aportando datos de amenaza a toda la solución, independientemente del origen.				
	6. Colaboración con comunidad de código abierto	Colaboración con la comunidad de código abierto para la amplia visibilidad de amenazas y la innovación de seguridad.				
	7. Análisis basado en	Soporte la inteligencia de				

	DNS	amenazas basada en análisis DNS.				
7.	**Detección y remediación avanzada de Malware**					
	1. Integración para análisis dinámico y estático	La solución deberá contar con integración a un ambiente virtual de análisis dinámico y estático para inspeccionar el Malware y poder identificar incluso Malware de tipo día cero. Preferiblemente tendrá la capacidad de poder integrar con la solución de endpoint para proveer un historial completo de cada paso ejecutado en los usuarios finales y/o servidores (endpoints) en donde el malware se encuentre localizado y deberá de tener la capacidad de remediarlo.				
	2. Actualización de base de datos de amenazas	El proceso de actualización de la base de datos de amenazas/vulnerabilidades y otros aspectos del mantenimiento (como parches y upgrades) deberá ser mediante el sitio Web del fabricante del producto y de varias formas: por medio del propio producto manualmente, bajando del sitio Web un archivo de actualización y de manera automatizada (pudiendo programar esta última con una frecuencia determinada).				
	3. Interacción con muestras analizadas	La solución de máquinas virtuales deberá permitir la interacción con las muestras analizadas de manera manual, permitiendo de esta manera descubrir comportamientos adicionales.				
	4. Suscripción para analizar archivos tipo Office, PDF, etc	La solución de máquinas virtuales deberá contar con una suscripción que también permita el envío de muestras manual, y con la que se				

		puedan analizar archivos de tipo Office, PDF, Flash, ejecutables, DLL, archivos comprimidos, así como URL para identificar malware en estos elementos.				
	5. Interface API	La solución virtual deberá proveer una interface API que permita realizar integraciones con desarrollos propios o con otras herramientas.				
	6. Entrega de evidencias	El ambiente de pruebas virtuales deberá de permitir la entrega de todas las evidencias de malware encontradas en un archivo que pueda utilizarse en un análisis forense posterior.				
	7. Notificaciones sobre contenido malicioso	Notificación retrospectiva sobre contenido de archivos maliciosos.				
	8. Proveer mapa visual de trayectoria	Capacidad de proveer un mapa visual de trayectoria de un archivo malicioso en el tiempo, mostrando el host de entrada, movimientos laterales y aplicación/protocolo utilizados por el ataque.				
	9. Soporte a varias ubicaciones del sistema sandbox	Soporte a sistema de sandbox local o en la nube				
8. Filtrado URL						
	1. Categorias URL soportadas	Soporte a más de 80 categorías				
	2. URL clasificadas	Más de 280 millones de URLs clasificadas				
	3. Actualizaciones en tiempo real	La solución permite actualizaciones en tiempo real a través de la nube u otro mecanismo.				
	4. URLs personalizadas	Las listas de URL personalizadas permiten que las URL formen parte de varias categorías.				
	5. Re categorización interactiva	La solución permite a los usuarios enviar la re-				

		categorización interactivamente, con un permiso o aprobación.				
	6. Búsqueda segura	La solución debe hacer cumplir una búsqueda segura				
	7. Excepciones a regla	La solución permite a los administradores permitir a los grupos o usuarios pasar por alto las reglas a un nivel granular sin acción administrativa de TI.				
9. Integración						
	1. Monitoreo via SNMP	Posibilidad de ser monitoreado por SNMP.				
	2. Manejo via SNMP	Posibilidad de ser manejado por SNMP.				
	3. Salida a SIEM	API para salida de eventos a SIEM.				
	4. Exploración de vulnerabilidades	API para la entrada de datos de conciencia ambiental (exploración de vulnerabilidades, perfiles de host).				
	5. Instrucciones a terceros	API para proporcionar instrucción a productos de terceros para la remediación automatizada.				
	6. Compatibilidad con protocolos estándar	Compatibilidad con protocolos estándar como NetFlow y WCCP.				
Plataforma de Gestión						
	1. Perfil para identificación de dispositivos móviles	El dispositivo debe tener la capacidad de construir un perfil para la identificación de dispositivos móviles, para lo cual debe incluir la siguiente información: sistema operativo, vulnerabilidades, aplicaciones. (sin necesidad de hardware o software separado).				
	2. Informes detallados y personalizables	Informes detallados y totalmente personalizables.				
	3. Generación de informes desde panel de control	Generación de informes de un solo clic desde el panel de control personalizable.				

	4. Acceso en base a roles	Control de acceso basado en roles y administración.				
	5. Métodos de autenticación	Autenticación externa (RADIUS, LDAP).				
	6. Búsquedas en eventos	Capacidad de ejecución de búsquedas en la base de datos de eventos				
	7. Crear y guardar búsquedas	Capacidad para crear y guardar búsquedas personalizadas - en todo el sistema y privadas.				
	8. Tableros personalizables	Tableros de control personalizados por usuario, incluidos widgets altamente personalizables.				
	9. Actualización de vulnerabilidades	El proceso de actualización de vulnerabilidades y otros aspectos del mantenimiento (como parches y upgrades) deberán ser mediante el sitio web del fabricante del producto y de varias formas: por medio del propio producto, bajando del sitio web un archivo de actualización o en forma automática.				
	10. Formatos de informes	Varios formatos de informes (PDF, CSV, HTML).				
	11. Flujo de trabajo personalizable	Generación de flujo de trabajo personalizado para análisis forenses rápidos.				
	12. Tablas personalizables	Generación de tablas personalizables y personalizables para agregar eventos dispares en una única vista.				
	13. Plataforma de gestión centralizada	Plataforma de gestión única para NGFW, NGIPS, análisis de clientes de punto final y generación de informes.				
	14. Multiples condiciones	La correlación de múltiples condiciones puede activar llamadas externas a dispositivos de terceros para la corrección.				
	15. Acceso via SQL	Acceso SQL externo a la base				

	externo	de datos para informes personalizados para herramientas como Crystal Reports.				

Instalación:

Deberán incluirse las labores de instalación, configuración y pruebas en el centro de datos principal del IHSS.

LOTE 2: EQUIPOS SWITCHES DE ACCESO PARA LA RED LAN DEL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

Adquisición de equipos de comunicaciones Switches de Acceso para la Red LAN del IHSS, en sus edificios principales:

La propuesta debe incluir:

1. Equipos
2. Servicios de instalación y configuración
3. Soporte Técnico por un año
4. Garantía estándar del fabricante por un año.

Equipos:

Descripcion	Cantidad
Switch Tipo 1	**10**
Switch Tipo 2	**30**

GENERALES:

Se desean adquirir, instalar y habilitar los switches de acceso en las siguientes localidades del IHSS: Hospital de Especialidades en Tegucigalpa, Campus del Edificio Administrativo en Barrio Abajo, Tegucigalpa, y en el Edificio del Hospital Regional de Norte en San Pedro Sula. Quedando de la siguiente manera:

El proveedor deberá suministrar, instalar y poner en operación los equipos de telecomunicaciones en base a la configuración propuesta por el IHSS; las actividades que deberán estar incluidas son:

- Montar y fijar los equipos de telecomunicaciones en los racks o gabinetes;
- Energizar los equipos;
- Realizar la desconexión de patchcords de los equipos actuales y conectarlos a los equipos que se suministre.
- Realizar la migración o configuración a los nuevos equipos a suministrar.
- Validar pruebas de conexión en conjunto con personal del área de Infraestructura de la Gerencia de Tecnologías de Información y Comunicaciones.

DESCRIPCIÓN DEL SERVICIO:

1. Durante la vigencia del contrato de soporte el proveedor deberá colaborar en realizar las configuraciones necesarias por el IHSS en los equipos provistos en conjunto con el Área de Infraestructura de la Gerencia de Tecnologías de Información y Comunicaciones.
2. Apoyará al IHSS para la buena operación de los equipos de telecomunicaciones y deberá reemplazar los equipos o componentes que sean necesarias durante la vigencia de la garantía.
3. Se proporcionará soporte técnico telefónico, remoto o en sitio cuando los incidentes presentados así lo ameriten.
4. Proporcionará un número telefónico directo y correo electrónico para recibir las solicitudes de soporte técnico.

5. Deberá atender y solucionar cualquier incidente reportado, atendiendo en un máximo de 2 horas y resolviendo según el caso en un máximo de 24 horas, sustitución del equipo o brindando alguna alternativa de solución.
6. Entregar una matriz de escalamiento de problemas con nombres, teléfonos fijo o celular y direcciones de correo electrónico.
7. La infraestructura de red del IHSS está basada protocolos estándares de la industria, por lo que las configuraciones deberán de poderse integrar a la infraestructura existente e instalada sin deteriorar los servicios de comunicaciones.
8. La empresa deberá entregar nota del fabricante de la solución donde se indique que esta cuenta con la capacidad técnica y el respaldo de la marca y del fabricante para el tipo de implementación de productos y servicios descritos en el LOTE 2: EQUIPOS SWITCHES DE ACCESO PARA LA RED LAN DEL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

CARACTERISTICAS DE LOS EQUIPOS DE COMUNICACIÓN

ESPECIFICACIONES GENERALES DE LOS EQUIPOS	
Garantía	Los equipos deberán contar con garantía de fabricante mínima de un año (1).
Soporte	Los equipos deberán contar con soporte técnico local o remoto en los casos que amerite durante un año. Este contrato debe incluir la configuración inicial y puesta en producción del equipo en el sitio, resolución de fallos y requerimientos adicionales en las configuraciones.
Accesorios	Para todos los puertos deberán incluirse los patchcords de fibra óptica de 3 pies de longitud (después de adjudicado se hará revisión de los tipos de conectores a usar). Así mismo se deberá incluir: • Los accesorios necesarios para la realización de instalación de equipos. • Los cables de conexión eléctrica AC • Documentación del equipo en físico o electrónico. • Al menos 1 Modulo FO (SFP+) para cada uno de los equipos switches a suministrar.

ESPECIFICACIONES TECNICAS MINIMAS						
SWITCH TIPO 1						
1	**General**	**Descripción**	**Cumple**		**Folio**	**Observación**
			Si	**No**		
	1. Tipo de dispositivo	Switch de acceso con 24 puertos ethernet 10/100/1000; 4 puertos de fibra óptica SFP+ - L2 – Gestionado.				
	2. Cantidad	10				

	3. Tipo incluido	Montaje en rack				
	4. Interfaces de conectividad a la red	Ethernet (RJ45) Small Form Factor Pluggable Plus (SFP+)				
	5. Puertos	• 24 puertos - Ethernet (RJ45) con 1 Gbps de velocidad • 4 puertos - Small Form Factor Pluggable Plus (SFP+) con 10 Gbps de velocidad				
	6. Rendimiento	Reenvio de ancho de banda: 1G (26 Gbps), 10G (64 Gbps) Cambio de ancho de banda: 1G (54 Gbps), 10G (120 Gbps) Velocidad de reenvío : 41 Mpps				
	7. Tamaño de tabla de dirección MAC	8k de entradas				
	8. Soporte para IPv4	Si (rutas unicast directas: 540, indirectas 250)				
	9. Soporte para IPv6	Si (rutas unicast directas: 410, indirectas 125)				
	10. Admite carcasa Jumbo	Si (10,200 bytes)				
	11. Capacidad máxima de VLANs activas	62				
	12. Protocolo de direccionamiento	RIP-1, RIP-2, direccionamiento IP estático, RIPng				
	13. Protocolo de gestión remota	SNMPv1, SNMPv2, SNMPv3, RMON 1, RMON 2, Telnet, SSH, CLI				
	14. Método de autentificación	Kerberos, Secure Shell (SSH), RADIUS, TACACS+				
	15. Características	Control de flujo, capacidad duplex, autosensor por dispositivo, Encaminamiento IP,				

		soporte de DHCP, negociación automática, soporte ARP, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), snooping IGMP, limitación de tráfico, admite Rapid Spanning Tree Protocol (RSTP), admite Multiple Spanning Tree Protocol (MSTP), soporte de Trivial File Transfer Protocol (TFTP), soporte de Access Control List (ACL), Quality of Service (QoS), soporte RADIUS, compatibilidad con Jumbo Frames, Rapid Per-VLAN Spanning Tree (PVRST), Protocolo de control de adición de enlaces (LACP)				
	16. Cumplimiento de estándares	IEEE 802.1D Spanning Tree Protocol IEEE 802.1p CoS Prioritization IEEE 802.1Q VLAN IEEE 802.1s IEEE 802.1w IEEE 802.1X IEEE 802.1ab (LLDP) Bluetooth Ver 4.0 IEEE 802.3ad IEEE 802.3af and IEEE 802.3at IEEE 802.3ah (100BASE-X single/multimode fiber only) IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-X RMON I and II standards SNMP v1, v2c, and v3 IEEE 802.3az IEEE 802.3ae 10 Gigabit Ethernet				

		IEEE 802.1ax				
	17. Memoria DRAM	512 MB				
	18. Memoria Flash	256 MB				
	19. Indicadores de estado	Estado del suministro de energía. RPS suministro de energía redundante.				
2.	**Expansión / Conectividad**					
	1. Interfaces	1 x consola - RJ-45 - gestión 1 x consola – USB - gestion 24 x RJ45 – 1 Gbps 4 x SFP+ - 10 Gbps (uplinks)				
3.	**Alimentación**					
	1. Dispositivo de alimentación	Fuente de alimentación eléctrica				
	2. Voltaje necesario	CA 120/230 V (50/60 Hz)				
	3. Consumo eléctrico en funcionamiento	120 vatios				
	4. Características	Conector de sistema de alimentación redundante (RPS)				
4.	**Diverso**					
	1. MTBF (tiempo medio entre errores)	2,400,000 horas				
	2. Cumplimiento de normas	Certificado FCC Clase A, TUV GS, cUL, EN 60950, EN55022, IEC 60950, EN55024, UL 60950 Third Edition, CISPR 22, CSA 22.2 No. 60950, FCC Part 15, AS/NZS 3548				

ESPECIFICACIONES TECNICAS MINIMAS

SWITCH TIPO 2						
1	**General**	**Descripción**	**Cumple**		**Folio**	**Observación**
			Si	**No**		

ESPECIFICACIONES TECNICAS MINIMAS

SWITCH TIPO 2						
1. General		**Descripción**	**Cumple**			
			Si	**No**	**Folio**	**Observación**
	1. Tipo de dispositivo	Switch de acceso con 48 puertos ethernet 10/100/1000; 4 puertos de fibra óptica SFP+ - L2 – Gestionado.				
	2. Cantidad	30				
	3. Tipo incluido	Montaje en rack				
	4. Interfaces de conectividad a la red	Ethernet (RJ45) Small Form Factor Pluggable Plus (SFP+)				
	5. Puertos	• 48 puertos - Ethernet (RJ45) con 1 Gbps de velocidad • 4 puertos - Small Form Factor Pluggable Plus (SFP+) con 10 Gbps de velocidad				
	6. Rendimiento	Reenvio de ancho de banda: 1G (50 Gbps), 10G (86 Gbps) Cambio de ancho de banda: 1G (102 Gbps), 10G (174 Gbps) Velocidad de reenvío : 76 Mpps				
	7. Tamaño de tabla de dirección MAC	8k de entradas				
	8. Soporte para IPv4	Si (rutas unicast directas: 540, indirectas 250)				
	9. Soporte para IPv6	Si (rutas unicast directas: 410, indirectas 125)				
	10. Admite carcasa	Si (10,200 bytes)				

	Jumbo					
	11. Capacidad máxima de VLANs activas	62				
	12. Protocolo de direccionamiento	RIP-1, RIP-2, direccionamiento IP estático, RIPng				
	13. Protocolo de gestión remota	SNMPv1, SNMPv2, SNMPv3, RMON 1, RMON 2, Telnet, SSH, CLI				
	14. Método de autentificación	Kerberos, Secure Shell (SSH), RADIUS, TACACS+				
	15. Características	Control de flujo, capacidad duplex, autosensor por dispositivo, Encaminamiento IP, soporte de DHCP, negociación automática, soporte ARP, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), snooping IGMP, limitación de tráfico, admite Rapid Spanning Tree Protocol (RSTP), admite Multiple Spanning Tree Protocol (MSTP), soporte de Trivial File Transfer Protocol (TFTP), soporte de Access Control List (ACL), Quality of Service (QoS), soporte RADIUS, compatibilidad con Jumbo Frames, Rapid Per-VLAN Spanning Tree (PVRST), Protocolo de control de adición de enlaces (LACP)				
	16. Cumplimiento de estándares	IEEE 802.1D Spanning Tree Protocol IEEE 802.1p CoS Prioritization IEEE 802.1Q VLAN IEEE 802.1s IEEE 802.1w IEEE 802.1X IEEE 802.1ab (LLDP) Bluetooth Ver 4.0 IEEE 802.3ad IEEE 802.3af and IEEE 802.3at IEEE 802.3ah (100BASE-X				

		single/multimode fiber only) IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-X RMON I and II standards SNMP v1, v2c, and v3 IEEE 802.3az IEEE 802.3ae 10 Gigabit Ethernet IEEE 802.1ax				
	17. Memoria DRAM	512 MB				
	18. Memoria Flash	256 MB				
	19. Indicadores de estado	Estado del suministro de energía. RPS suministro de energía redundante.				
2.	**Expansión / Conectividad**					
	Interfaces	1 x consola - RJ-45 - gestión 1 x consola – USB - gestión 48 x RJ45 – 1 Gbps 4 x SFP+ - 10 Gbps (uplinks)				
3.	**Alimentación**					
	Dispositivo de alimentación	Fuente de alimentación eléctrica				
	Voltaje necesario	CA 120/230 V (50/60 Hz)				
	Consumo eléctrico en funcionamiento	120 vatios				
	Características	Conector de sistema de alimentación redundante (RPS)				
4.	**Diverso**					
	MTBF (tiempo medio entre errores)	1,350,000 horas				
	Cumplimiento de normas	Certificado FCC Clase A, TUV GS, cUL, EN 60950, EN55022, IEC 60950, EN55024, UL 60950 Third Edition, CISPR 22, CSA 22.2 No. 60950, FCC Part 15, AS/NZS 3548				

Visitas de campo:

En las visitas de campo a las instalaciones del IHSS en Tegucigalpa, el oferente podrá verificar y validar la compatibilidad de la infraestructura de comunicaciones del IHSS con el equipo ofertado.

Instalación:

Deberán incluirse las labores de instalación, configuración y pruebas en los edificios del IHSS en Tegucigalpa y San Pedro Sula.

Soporte Técnico:

Se deberá contar con servicio de soporte técnico estándar, que podrá ser contactado vía telefónica y vía correo electrónico.

LOTE 3: CERTIFICACION Y REPARACION DE CABLEADO DE FIBRA OPTICA (BACKBONE) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

El IHSS requiere los servicios de la certificación y reparación (en los casos que corresponda) del cableado de fibra óptica (backbone) de los siguientes edificios:

1. Campus del IHSS en Barrio Abajo, Tegucigalpa
    a. Edificio Administrativo
    b. Edificio Invalidez, Vejez y Muerte (IVM)
    c. Clinica Periferica 1
    d. Clinica de Adulto Mayor
2. Hospital de Especialidades en el Barrio La Granja, Comayagüela
3. Hospital de San Pedro Sula, Colonia Tara, San Pedro Sula

La propuesta debe incluir:

1. Limpieza exterior e interior de los gabinetes de distribución del cableado estructurado distribuidos en los diferentes edificios del IHSS.
2. Limpieza de conectores y adaptadores del cableado de fibra óptica actualmente instalado en los diferentes edificios del IHSS.
3. Diagnóstico y validación de la capacidad de cada uno de los enlaces de fibra óptica instalados en la red interna del IHSS.
4. Corrección/reparación de los enlaces de fibra óptica del backbone que presenten deficiencias en el diagnóstico y revisión preliminar realizado.
5. Certificación de la totalidad de los enlaces de fibra óptica de la instalación (desde cada extremo).
6. Suministro e instalación de 90 unidades de patch cords compatibles con la instalación existente, para reemplazar los actuales y tener en disponibilidad en caso de daño en alguna unidad. (Después de adjudicado se hará revisión de los tipos de conectores a usar, ya que los lotes 2 y 3 son relacionados y dependientes).

Descripción de la Instalación actual del IHSS:

El cableado de fibra óptica (backbone) de los edificios del IHSS está compuesto de los siguientes componentes:

1. CABLEADO DE FIBRA OPTICA.
   Es del tipo Multimodo, 50/125µm, OM2. (cada cable de fibra óptica hacia cada gabinete está compuesta por 6 hilos dentro de cada uno).
2. CONECTORES DE FIBRA ÓPTICA.
   Son del tipo pre-pulido, interface SC, 50/125µm, OM2.
3. DISTRIBUIDORES DE FIBRA ÓPTICA
   Cada gabinete de distribución, cuenta con un distribuidor de fibra óptica, con 3 conexiones cada una.
4. CANALIZACIONES
   En general el cableado cuenta con canalizaciones, escalerillas y ductos por donde se encuentra alojada la fibra óptica y distribuida al resto del backbone.

5. Se tienen identificados 96 hilos de fibra óptica (16 enlaces), que no estan brindando servicios de conectividad a los equipos de comunicaciones, los cuales las causas pueden variar, ya sea un corte, quiebre, suciedad en algun componente.

Prueba del Sistema:

Para la validación de las pérdidas de los enlaces de fibra óptica se solicita que los certificadores estén calibrados al menos dentro de un período un año y que tenga su certificado de calibración correspondiente cuando corresponda. Deberá presentarse evidencia del certificado vigente.

Las pruebas pueden realizarse utilizando los siguientes equipos:

- Certificadores de fibra óptica.
- Medidores de pérdidas, siempre que puedan entregarse los datos en formato PDF.
- OTDR.

En cualquiera de los equipos a utilizar debe de estar debidamente calibrado y certificado por el fabricante o distribuidor autorizado local.

Patch Cords de Fibra Óptica a proveer:

1. Cantidad: 90 unidades
2. Tipo: 50/125µm, OM3
3. Longitud: 1 metro.
4. Terminación 1: SC, dúplex
5. Terminación 2: LC, dúplex
6. Tipo de chaqueta: NEC OFNR.
7. Standard: ANSI/TIA-568C.3

(Después de adjudicado se hará revisión de los tipos de conectores a usar, ya que los lotes 2 y 3 son relacionados y dependientes).

Hilos de cableado de fibra óptica por cada localidad:

Sitio	Hilos con actividad	Hilos a Reparar (dañados)	Total por certificar por sitio
Edificio Administrativo TGU	72	0	72
Edificio IVM	24	0	24
Clínica Periférica 1	30	12	42
Clínica de Adulto Mayor	6	0	6
Hospital de Especialidades, TGU	30	60	90
Hospital Regional del Norte, SPS	66	24	90
TOTAL	**228**	**96**	**324**

NOTA: Los hilos a reparar también deben de ser certificados.

Visita de Campo:

En las visitas de campo a las instalaciones del IHSS en Tegucigalpa y San Pedro Sula, el oferente podrá verificar y validar el estado de la red de cableado de fibra óptica en cada sitio, para que en base a esta pueda identificar elementos adicionales que requiera para que pueda presentar la propuesta.

Requisito técnico:

La empresa deberá entregar constancia de proyectos similares realizados a los descritos en el LOTE 3: CERTIFICACION Y REPARACION DE CABLEADO DE FIBRA OPTICA (BACKBONE) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

LOTE 4: SOLUCION DE FIREWALL DE SEGURIDAD PERIMETRAL DE PROXIMA GENERACION PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

El IHSS requiere de la adquisición de una solución de seguridad perimetral comprendida por un firewall de próxima generación con módulos de gestión y monitoreo, para ser utilizado en su Centro de datos principal en Tegucigalpa.

La propuesta debe incluir:

Equipo de Seguridad perimetral integrado que incluye:

- Componente de seguridad perimetral (dispositivo, softwares y servicios), incluyendo componentes y accesorios necesarios para su puesta en producción.
- Componente de administración y monitoreo (dispositivo, softwares y servicios); incluyendo componentes y accesorios necesarios para su puesta en producción.
- Servicios de Instalación, configuración, pruebas, verificación del correcto funcionamiento de la solución de infraestructura, equipos, componentes y su software de gestión.
- Servicios de Capacitación por parte del representante del fabricante en el uso, administración, configuración y monitoreo de la solución adquirida para el Área de Infraestructura de la Gerencia de IT del IHSS, para seis personas un mínimo.
- Servicio de garantía del fabricante: los equipos, todos sus componentes de hardware y software deben de tener una garantía 1 año como mínimo.
- Servicios de Suscripción con el fabricante por un año: el equipo deberá contar con una suscripción para descarga de archivos de definiciones de manera automática para todos los componentes de la solución, la cual deberá incluir soporte técnico (local y remoto cuando fuera necesario), actualizaciones y corrección de errores.
- El proveedor deberá incluir todos los accesorios, medios, equipos, etc que sean necesarios para la puesta en producción del equipo.
- La empresa deberá entregar nota del fabricante de la solución donde se indique que esta cuenta con la capacidad técnica y el respaldo de la marca y del fabricante para el tipo de implementación de productos y servicios descritos en el LOTE 4: SOLUCION DE FIREWALL DE SEGURIDAD PERIMETRAL DE PROXIMA GENERACION PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

Especificaciones Técnicas Mínimas:

Especificación		Descripción	Cumple		Folio	Observación
REQUERIMIENTOS GENERALES			**Si**	**No**		
Solución de Seguridad Perimetral de nivel empresarial		**Solución de seguridad perimetral empresarial (hardware y software), de alto rendimiento y capacidades de última generación con capacidades de administración y monitoreo.**				
	Cantidad:	1				
	1. La solución debe poder	a. Modulo Firewall b. Módulo de Prevención de				

	incluir las siguientes características	Intrusión (IPS) c. Adquisición de Identidad de Usuario d. Módulo de Control de Aplicaciones e. Módulo de Filtrado WEB f. Modulo Anti-Bot g. Modulo Antivirus / Antimalware h. Emulación y Extracción de Amenazas. i. IPSec VPN				
	2. Interface Lights-Out-Management (LOM)	El dispositivo debe poseer una interface Lights-Out-Management (LOM) para diagnóstico remoto con la posibilidad de iniciar, reiniciar y gestionar el appliance desde una locación remota				
	3. Interfaces de conexión	8 interfaces 10/100/1000Base-T (RJ45) 2 interfaces 10GBase-F SFP+				
	4. Métodos de conexión a la administracion	El equipo debe ser accesible a través de SSH, cliente o a través de una interfaz Web usando SSL.				
	5. Capacidad de Almacenamiento	El equipo debe tener almacenamiento con redundancia en sus discos duros, con capacidad de al menos 2x500 GB (RAID1).				
	6. Redundancia de Energía	El equipo debe incluir fuentes de poder redundantes con tecnología hot swappable.				
	7. Memoria RAM	64 GB				
	8. Procesador	1 CPU, 8 Cores físicos				
	9. Formato	El equipo debe poder ser instalado en rack estándar (debe incluir los accesorios de instalación)				
	10. Throughput de IPS	El throughput del IPS activo, dentro de la misma plataforma con tráfico mixto debe ser de al menos 4.5 Gbps en condiciones de producción.				
	11. Throughput de Firewall	El throughput de Firewall debe ser de al menos 30 Gbps en condiciones de producción.				
	12. NGFW Throughput	3 Gbps en condiciones de produccion, teniendo activados				

		los módulos de Control de Aplicaciones, IPS y el Firewall				
	13. Conexiones Concurrentes	Debe soportar al menos 3 millones de conexiones concurrentes.				
	14. Sistema Operativo	El Sistema Operativo debe estar totalmente adaptado para direccionamiento IPv4 e IPv6.				
	15. Modo	Debe soportar Link Aggregation (802.3ad) en modo pasivo y activo.				
	16. Implementación	Debe Soportar implementación en modo transparente (Layer 2) o en modo ruteo (Layer 3)				
	17. Copias de seguridad	La solución debe ser capaz de realizar copias de respaldo y restauración de la configuración, permitiendo al administrador configurar la realización de copias en el tiempo deseado.				
	18. Alojamiento de copias	Los archivos de copias de seguridad pueden ser almacenados localmente y/o en un equipo remoto.				
	19. Alta Disponibilidad (HA)	La solución debe tener la posibilidad de soportar la configuración y funcionalidad de alta disponibilidad, la compartición de carga con sincronización de estad sus modos de operación (Activo-Activo o Activo Pasivo) para proyecto un futuro.				
	20. Alta Disponibilidad ISP	Capacidad de hacer disponibilidad de al menos 3 conexiones a internet con diferentes ISPs, configurable ya sea manual o automática, en modo activo/pasivo o activo/activo.				
	21. Dispositivo hardware certificado	El dispositivo de hardware sobre el que deberá ejecutarse la solución de seguridad perimetral deberá estar certificado y garantizado del correcto funcionamiento del software por parte del fabricante de la solución.				
REQUERIMIENTOS TECNICOS ESPECIFICOS						
Solución de Firewall						

1	**Modulo Firewall**	**El modulo firewall de la solución perimetral deberá poder monitorear el tráfico de red - entrante y saliente - y decidir si permite o bloquea tráfico específico en función del conjunto de reglas de seguridad definidas en la solución.**				
	1. Tecnología Stateful inspection	El modulo firewall debe estar basado en la tecnología conocida como "Stateful inspection", la cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del Gateway, y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos.				
	2. Controles de Acceso	Debe permitir crear controles de acceso a por lo menos 150 aplicaciones/servicios/protocolos predefinidos.				
	3. Parámetros de origen y destino	Debe tener la opción de negar los parámetros de origen o destino, es decir que para una regla dada permite todas las conexiones de origen / destino excepto la especificada en la regla.				
	4. Implementacion de Reglas a intervalos de tiempo.	Debe permitir implementar reglas aplicadas a intervalos de tiempo específicos, con la finalidad de definir el momento exacto en que una regla toma acción o expira.				
	5. Network Address Translation (NAT)	Debe incluir la posibilidad de crear NATs dinámicos (N-1 o Hide) y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete y en una sola regla.				
	6. Autenticación de Usuarios	El firewall debe soportar varios métodos de autenticación, al				

		menos por usuario, por un cliente (a través de la dirección IP) y por sesión.				
	7. Modo Transparente	El firewall debe permitir poder conectarse de modo transparente (bridge Mode).				
	8. Soporte Bootp/DHCP Relay	Debe soportar Bootp/DHCP Relay				
	9. Sumarizaciónde rutas	Debe soportar sumarización de rutas (route aggregation) y redistribución de rutas a otros protocolos (route redistribution).				
	10. Ruteo Dinámico RIP	Debe soportar ruteo dinámico con RIP versión 2, OSPFv2, y BGP versión 4. Estos 3 protocolos deben ser soportados también en IPv6				
	11. Control de Ancho de Banda	Debe soportar control de ancho de banda basado en prioridades de pesos				
	12. Servicios Diferenciados Integrados	Debe soportar servicios diferenciados integrados (DiffServ)				
	13. Mecanismos de detección de engaño	Debe tener mecanismos de detección de engaños de IP, donde paquetes externos a la red usan direcciones internas para saltarse los controles de seguridad.				
	14. Monitoreo de Alta Disponibilidad	La consola de administración también debe permitir monitorear el estado de la alta disponibilidad.				
2	**Módulo de Prevención de Intrusión (IPS)**	**El modulo Sistema de Prevención de Intrusos (IPS) debe estar integrado en la solución perimetral y debe proteger la red de perímetro y el ingreso a la red interna desde internet de ataques, abusos o actividades maliciosas. El módulo IPS deberá ser capaz de tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o**				

		puertos.				
	1. El módulo IPS debe incluir:	El IPS integrado, debe incluir al menos los siguientes mecanismos de defensa: a. Protecciones que contienen ajustes que alteran el comportamiento de otras protecciones. b. Anomalías de protocolo: grupo de protecciones que identifican cuando el tráfico no cumple con los estándares del protocolo. c. Firmas: grupo de protecciones que identifica el tráfico que intenta explotar una vulnerabilidad específica d. Control de aplicaciones: Previene el uso de aplicaciones específicas del usuario. e. Debe proveer cobertura de protecciones para amenazas de clientes, servidores, sistemas operativos, infecciones de malware y gusanos.				
	2. Fail Open	El IPS debe tener un software basado en el mecanismo de Fail Open.				
	3. Actualización de firmas	El IPS debe ofrecer un mecanismo automatizado para activar o administrar nuevas firmas a partir de las actualizaciones.				
	4. Inspección de trafico SSL	El IPS debe poder inspeccionar el tráfico SSL				
	5. Configuración de Excepciones	El IPS debe soportar la configuración de excepciones basadas en la fuente, destino, servicio o una combinación de los tres.				
	6. Correlación y Eventos	El módulo de IPS debe tener un mecanismo de correlación y reporte centralizado de eventos.				
	7. Bypass por sobre carga	Debe soportar software configurable para realizar bypass en caso de alta carga, para garantizar rendimiento de				

		red.				
	8. Protección DoS	Debe tener protección contra ataques DoS				
	9. Detección y Prevención	El IPS debe ser capaz de detectar y prevenir las siguientes amenazas: desuso de protocolo, comunicaciones maliciosas, intentos de tunelización y tipos de ataques genéricos sin firmas predefinidas.				
	10. Captura de paquete	El IPS debe ser capaz de realizar captura del paquete para protecciones específicas.				
	11. Detección y bloqueo	El IPS debe ser capaz de detectar y bloquear los ataques de la capa de red y aplicación, protegiendo por lo menos los siguientes servicios: servicios de correo electrónico, DNS, FTP, servicios Windows (Microsoft Networking), SNMP, HTTP e ICMP.				
	12. Exclusiones	El administrador debe ser capaz de definir las exclusiones de redes y host de la inspección del IPS.				
	13. Cache DNS	La solución debe proteger del Envenenamiento de Caché DNS y prevenir a los usuarios el acceso a direcciones de dominio bloqueadas.				
	14. Bloqueo de Control Remoto	El IPS y/o el Control de Aplicaciones deben detectar y bloquear las aplicaciones de controles remotos, incluyendo aquellos que son capaces de tunelizar sobre el tráfico HTTP.				
	15. Protocolo CITRIX	La solución debe cumplir la ejecución del protocolo Citrix.				
	16. Bloqueo de trafico	La solución debe permitir al administrador bloquear fácilmente el tráfico de entrada y/o de salida.				
	17. Inspección de HTTPS	Debe soportar Inspección de tráfico encriptado HTTPS tanto Inbound como Outbound. Sin				

		necesidad de HW dedicado externo.				
	18. Excepciones en base a eventos	Debe permitir la creación de excepciones a partir de los eventos reportados.				
	19. Estado de Servicios de Inspección y Bloqueo	El IPS integrado, debe incluir la habilidad de detener temporalmente la inspección y bloqueo en el gateway, para efectos de “troubleshooting”.				
	20. Trafico P2P	Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambió de puertos. El administrador debe poder definir objetos de red y servicios a excluir.				
	21. Soporte de Protocolos VoIP	Debe soportar y proteger protocolos de VoIP (H.323, SIP, MGP y SCCP), asegurando que todos los paquetes de VoIP son estructuralmente válidos.				
	22. Bloqueo de trafico geo localizado	Debe permitir bloquear tráfico entrante, saliente o ambos correspondientes a determinados países, sin necesidad de actualizar manualmente los rangos IP correspondientes a cada país.				
	23. Gestión de tabla de conexiones y memoria	Con el fin de incrementar la estabilidad del Gateway de IPS, debe brindar un mecanismo que sea capaz de administrar la capacidad de la tabla de conexiones y el consumo de la memoria del Gateway, esto permitirá al Gateway manejar grandes cantidades de tráfico inesperado, por ejemplo en ataques de denegación de servicio.				
	24. Aplicación de nuevas protecciones	El IPS debe poder aplicar nuevas protecciones al mismo tiempo que protege la red de ataques. Con protección en tiempo real y actualizaciones de protecciones para:				

		vulnerabilidades, malware, tunneling, control de aplicaciones y ataques genéricos.				
	25. Análisis forense	Debe ser capaz de realizar captura de tráfico para análisis forense.				
3	**Adquisición de Identidad de Usuario**	**La solución de seguridad perimetral deberá ser capaz de adquirir la identidad de los usuarios que hagan uso de los servicios de conexión a internet y otros servicios que brinde la solución.**				
	1. Integración con Servicios de Directorio Activo	El Gateway debe ser capaz de integrarse a los servicios de Directorio Activo de Microsoft y adquirir la identidad de los usuarios autenticados en los equipos clientes.				
	2. IP-Spoofing y Identity-Spoofing	La solución debe proteger a los clientes de ataques IP-spoofing y Identity-Spoofing.				
	3. Esquemas de autenticación	Debe soportar el uso de varios esquemas de autenticación, como ser tokens, TACACS, RADIUS, certificados digitales.				
	4. Grupos LDAP	La solución debe soportar el uso de grupos alojados de LDAP.				
	5. Reglas de acceso por usuarios o grupos	Con la finalidad de crear reglas de acceso por usuarios o grupos, debe poder integrase con otras soluciones como: control de aplicaciones y filtrado de URL o filtrado de contenido.				
	6. Retención de identidad	La solución debe retener la identidad de los usuarios aun cuando estos cambien la dirección IP del equipo cliente.				
	7. Sistemas operativos soportados	La autenticación de los clientes y/o usuarios puede ser a través de sistemas operativos Windows, Linux, Mac OS, etc.				
4	**Módulo de Control de Aplicaciones**	**El Módulo de Control de Aplicaciones de deberá estar integrada en la solución de seguridad perimetral y deberá tener la posibilidad de**				

		controlar y limitar el uso de las aplicaciones y mantener alejadas de la red institucional las aplicaciones improductivas, inapropiadas y peligrosas.				
	1. Aplicaciones por defecto	La solución debe contar con una base de datos de más de 6,000 aplicaciones diferentes y más de 250,000 widgets web 2.0 como mensajería instantánea, redes sociales video streaming, VoIP, juegos, entre otros.				
	2. Creación de objetos	La solución debe permitir la creación de objetos de tiempo por aplicación o grupo de aplicaciones en las reglas, para que una acción definida se cumpla sólo durante tiempos especificados.				
	3. Inspección de trafico HTTPS	Debe inspeccionar el tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo SSL.				
	4. Clasificación de aplicaciones	Debe tener un servicio de clasificación basando en la nube que permita categorizar dinámicamente el tráfico Web.				
	5. Integración con servicios de Directorio Activo	Debe ser posible integrar la solución con Directorio Activo u Open LDAP para crear reglas de control de aplicaciones y filtrado URL basadas en: usuarios, grupos de Usuarios, maquinas, dirección IP, redes y todas las opciones combinadas.				
	6. Limitar ancho de banda por aplicación	La solución debe ofrecer un mecanismo para limitar el uso de las aplicaciones basado en el consumo del ancho de banda.				
	7. Integración de la solución	La solución debe ser capaz de integrar control de aplicaciones y filtrado de URL dentro de la misma plataforma que además proporcione una solución de firewall, IPS, etc.				
	8. Capacidad de	Capacidad para identificar,				

	Identificación WEB 2.0	permitir, bloquear o limitar el uso de las aplicaciones por usuario o grupos limitando de esta forma la web 2.0, redes sociales, independientemente del puerto o protocolo o técnica evasiva para atravesar la red.				
	9. Categorización de aplicaciones	Deberá contar con más de 150 categorías basadas en criterios como tipos de aplicaciones, nivel de riesgo de seguridad, uso de recursos e implicaciones de productividad.				
	10. Identificación de los usuarios	Deberá contar con un identificador de usuario el cual le permite enviar alertas a los usuarios en tiempo real acerca de sus limitaciones de acceso a aplicaciones.				
	11. Prevención de infecciones desde aplicaciones	Debe tener la capacidad de prevenir infecciones de malware provenientes de aplicaciones y widgets de redes sociales.				
5	**Módulo de Filtrado WEB**	**El Modulo de Filtrado de WEB integrada de la solución de seguridad perimetral deberá ser capaz de identificar determinados tipos de sitios web, como los sitios malintencionados conocidos o los sitios que muestran material inadecuado y deberá permitir o bloquear el acceso a los sitios en función de las categorías de direcciones URL predefinidas.**				
	1. Categorización de sitios WEB	Debe cubrir más de 200 millones de sitios web en al menos 60 categorías/sub categorías preconfiguradas, incluidas las siguientes: Adultos, anuncios, chat, criminal, drogas, juego, videojuegos, la piratería, proxies remotas, educación sexual, compras, deportes, streaming de medios de comunicación, la violencia, las armas, basado, redes sociales,				

		etc.				
	2. SafeSearch en motores de búsqueda.	El Modulo de Filtrado WEB debera de poder aplicar seguridad SafeSearch a los motores de búsqueda.				
	3. Filtrado de Sitios WEB 2.0	El Modulo de Filtrado WEB debe tener la capacidad de bloquear granularmente sitios basado en Web 2.0.				
	4. Configuración de reglas	La solución debe ser capaz de configurar reglas de filtrado con múltiples categorías.				
	5. Filtrado especifico	La solución debe ser capaz de crear un filtrado para un único sitio a ser soportado por múltiples categorías.				
	6. Filtrado granular	La solución debe tener granularidad de los usuarios y grupos con las normas de seguridad.				
	7. Excepciones de objetos	La solución debe permitir las excepciones de red basadas en los objetos de red definidos.				
	8. Invalidez de categoría	La solución debe ofrecer un mecanismo de invalidez en la categorización para la base de datos de la URL.				
	9. Inspección de trafico HTTPS	Debe inspeccionar el tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo SSL.				
	10. Bypass Proxy	El Filtrado WEB debe tener la capacidad de identificar y bloquear herramientas de “proxy bypass” sobre protocolos estándar y no estándar (sin la necesidad de instalar un agente en los hosts o licencias adicionales).				
	11. Identificación de usuarios	El Filtrado WEB deberá contar con un identificador de usuario el cual le permite enviar alertas a los usuarios en tiempo real acerca de sus limitaciones de acceso a sitios web.				
	12. Paginas	El módulo de Filtrado WEB				

	traducidas y en cache	deberá tener la capacidad de filtrar páginas traducidas y en cache.				
	13. Control granular	El modulo de Filtrado WEB deberá permitir control granular para aceptar, bloquear o limitar acceso basado en usuarios, grupos o máquinas para sitios específicos o categorías completas.				
	14. Autenticación mediante portal cautivo	La solución deberá permitir la autenticación de usuarios mediante un portal cautivo para aquellos usuarios que no están en el dominio, por ejemplo usuarios invitados.				
6	**Modulo Contra Botnets**	**La solución de seguridad perimetral debe contar de manera integrada con una herramienta que haga descubrimiento de botnets dentro de la red institucional. Dicha herramienta debe bloquear la comunicación que intenten establecer los botnets con los atacantes.**				
	1. Detección de host infectados	La solución debe poder detectar host internos infectados con botnets, analizando el tráfico de la red utilizando una tecnología multicapa.				
	2. Consultas a nube del fabricante	La solución debe proveer seguridad en tiempo real haciendo consultas a la nube de inteligencia del fabricante. La Base de datos debe contener un mínimo de 4 millones de firmas de malware.				
	3. Descubrimiento de botnets	La herramienta contra botnets debe analizar al menos 150 millones de direcciones para descubrimiento de bots, que incluyan al menos, direcciones de: IP de Command and Control, URL y DNS.				
	4. Prevención de robo de información	La herramienta contra botnets deberá prevenir daños de robo de información mediante el				

		bloqueo de las comunicaciones de las maquinas infectadas.				
	5. Patrones de comunicación	Debe incluir al menos 2000 patrones de comunicación de botnets.				
		La solución debe incluir al menos los siguientes métodos de identificación: • Identificación de DNS de Command and control utilizadas por los criminales para controlar los bots. • Identificación de patrones de comunicación utilizada por cada familia de bots.				
	6. Tecnologia de Inspección	La solución debe utilizar tecnología de inspección multicapas.				
7	**Modulo Antivirus / Antimalware**	**La solución de seguridad perimetral deberá contar de manera integrada con un Módulo Antivirus / Antimalware; que asegure que la red y los dispositivos permanecerán libres de malware utilizando motores de detección de amenazas avanzados y de múltiples capas para identificar y bloquear malware en la puerta de enlace de la red; proporcionando protección real contra virus, troyanos, gusanos, spyware y rogueware.**				
	1. Motor de inspección	El motor de inspección debe ser basado en firmas y análisis de comportamiento				
	2. Firmas de virus	El sistema de inspección debe contener más de 4 millones de firmas de virus y más de 250,000 sitios conocidos como fuentes de infección.				
	3. Escaneo de Protocolos	Escaneo de virus y bloquear por lo menos con base a los protocolos POP3, FTP, SMTP HTTP, HTTPS, IMAP, archivos de mensajería instantánea				

		protocolos P2P, y todos los principales formatos de archivos incluyendo archivos comprimidos.				
	4. Escaneo en tiempo real	El módulo de Antivirus / Antimalware debe hacer escaneo en tiempo real tanto de antivirus como de antimalware				
	5. Basado en patrones	Deberá basarse en patrones previniendo contra software espía y gusanos.				
	6. Acciones	Deberá permitir al administrador elegir la acción (block o pass) para al menos 70 diferentes tipos de archivos. La detección del tipo de archivo no debe ser basada en la extensión del mismo				
	7. Capacidad de escaneo	Capacidad para escanear archivos al menos de 2Gb de tamaño aun comprimidos, con la opción de configurar un tamaño más pequeño de archivo. El administrador puede decidir el límite de tamaño de archivo antes de bloquearlo, o pasarlo sin ningún tipo de scan.				
	8. Descompresión de archivos	Descompresión de archivos, con la opción de poder configurar el máximo nivel de anidación y de compresión para evitar ataques DoS.				
	9. Remoción de contenido malicioso	Debe soportar remover contenido malicioso de distintas partes de un documento, como mínimo: macros, objetos y archivos embedidos; y accesos URLs (links) a sitios externos.				
	10. Acciones ante falla	Deberá tomar acciones cuando el escaneo de archivos falle o exista sobre carga en el motor de antivirus.				
	11. Detección de dispositivos infectados	Detección dispositivos infectados con bots, analizando el tráfico de la red utilizando una tecnología multicapa.				
	12. Detección y	Detección y bloqueo de malware				

	bloqueo	desconocido, ataques dirigidos y ataques de día cero				
	13. Pre Infección	Detección y bloqueo de virus conocidos (Pre-infección) y transferencias de archivos				
	14. Post Infección	Detección y bloqueo de infección post-bot, prevención y la visibilidad de la amenaza				
	15. Inspección de Trafico encriptado	Debe hacer inspección sobre tráfico encriptado PPTP, L2TP, IPSec, SSL.				
	16. Políticas granulares	Debe soportar la configuración de políticas granulares basadas en IPs o usuarios.				
8	**Emulación y Mitigación de Amenazas.**	**La solución de Seguridad Perimetral debe contar con una capa de protección contra amenazas desconocidas mediante emulación de archivos (sandboxing) y la posibilidad de mitigación o eliminación de la amenaza detectada.**				
	1. Emulación de archivos	La solución debe contar con un sistema de emulación de archivos para búsqueda de Malware con opciones basadas en emulación en la nube y emulación local; de modo que al menos los documentos de Microsoft Office, PDFs, ejecutables y comprimidos (entre otros) puedan ser reconstruidos en el mismo dispositivo de seguridad, mitigando o eliminando cualquier malware en estos.				
	2. Ataques de día cero	Protección contra ataques de día cero: La solución debe proteger contra amenazas de día cero, antes de que la firma estática sea creada.				
	3. Prevención de ingreso	Debe prevenir archivos maliciosos antes de que lleguen a la red interna.				
	4. Ataques dirigidos	Debe proteger de ataques dirigidos a sistemas operativos Windows en múltiples versiones.				

	5. Tamaño de archivos	La solución debe emular archivos mayores de 10mb				
	6. Tipos de archivos	Debe soportar al menos los siguientes tipos de archivos: extensión ".exe", MS-Office, PDF, SCR, Java, Flash, msi y verificación aun dentro de archivos comprimidos.				
	7. Tipos de Protocolos	Debe soportar al menos los siguientes protocolos: HTTP, HTTPS, SMTP, CIFS, FTP				
	8. Comunicaciones cifradas	Debe soportar descifrado de archivos transferidos en una comunicación cifrada SSL o TSL dentro de la misma caja.				
	9. Políticas granulares	Debe soportar políticas granulares basadas en usuario				
	10. Reconstrucción de archivos	La solución debe ser capaz de reconstruir los archivos con los elementos que son seguros (imágenes, textos, tablas, entre otros)				
	11. Eliminar amenazas	La solución debe eliminar las amenazas y eliminar contenido explotable, incluyendo el contenido activo y objetos incrustados				
	12. Archivo en versión libre de amenaza	El archivo debe ser entregado inmediatamente en una versión libre de amenazas, con acceso a la original sólo después de que ha sido considerado seguro				
	13. Tipo de contenido	La solución debe mantener la flexibilidad con opciones de mantener el formato de archivo original y especificar el tipo de contenido que será eliminado.				
	14. Monitoreo e inspección	Se debe monitorear e inspeccionar la actividad y comportamiento que provoca el archivo inspeccionado en múltiples sistemas operativos y versiones de office.				
	15. Reportes	Se debe poder generar reportes detallados de la emulación, mitigación y eliminación de la amenaza.				

9	**IPSec VPN**	**La solución de seguridad perimetral debe incluir la posibilidad de recibir y configurar conexiones VPN con soporte a VPNs IPSec y VPNs SSL (conexiones clientes y túneles VPN). Las redes privadas virtuales (VPNs), deberán permitir a los usuarios conectarse de forma remota y segura a través de redes públicas, como si lo estuvieran haciendo a través de una red de área local (LAN)**				
	1. Autoridad de Certificación	La solucion debe tener la posibilidad de soportar tanto un CA Interno provisto por un tercero.				
	2. Validación de conexión VPN	Debe poder validar la conexión VPN por medio de certificados digitales o llaves secretas.				
	3. Algoritmos cifrados	Debe ser soportado 3DES y AES-256 para las fases I y II de IKE.				
	4. Protocolo Criptográfico	Debe soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit).				
	5. Integridad de datos	Debe soportar integridad de datos con md5 y sha1.				
	6. Topologías de conexión	Debe incluir soporte a las topologías VPNs site-to-site: Full Meshed (todos a todos), Star (Oficinas Remotas a Sitio Central) y Hub and Spoke (Sitio remoto a través del sitio central hacia otro sitio remoto)				
	7. Autenticación de usuarios	Verificación de usuarios con autenticación de dos (2) factores.				
	8. Verificación de cumplimiento de dispositivos	Debe incluir una función para la verificación de cumplimiento de requerimientos de seguridad mínimos de portátiles y Pcs.				
	9. Cliente VPN	Soporte a VPNs client-to-site basadas en IPSEC y SSL a través de cliente de instalación				

		(debe incluir la licencia tanto de cliente como del servicio). Tanto para sistemas operativos clientes Windows, Linux y MacOS.				
	10. Dispositivos Móviles	Soporte para acceso remoto a aplicaciones corporativas para dispositivos smartphones, tablets o PCs.				
	11. Configuración de reglas	El administrador debe poder aplicar reglas de control de tráfico, al interior de la VPN.				
Solución de Administración y Monitoreo Centralizada						
Módulo de Administración y Monitoreo		**La solución de administración y monitoreo centralizada de la solución deberá ser un dispositivo físicamente separado del dispositivo de seguridad.**				
	1. Cantidad	1				
	2. Requerimiento de administración y monitoreo de la solución.	Deberá tener las siguientes funcionalidades: a. Administración de la política de seguridad b. Identificación de Usuarios c. Módulo de Monitoreo d. Visualizador de Eventos y Reportes e. Repositorio de registros y eventos de seguridad				
	3. Dispositivo	Las funcionalidades descritas en este apartado, deberán estar alojados y ejecutándose en un único dispositivo adicional; sin embargo el software es				
	4. Interface Lights-Out-Management (LOM)	El dispositivo debe poseer una interface Lights-Out-Management (LOM) para diagnóstico remoto con la posibilidad de iniciar, reiniciar y gestionar el appliance desde una locación remota				
	5. Interfaces de conexión	4 interfaces 10/100/1000Base-T (RJ45)				
	6. Métodos de conexión a la administración y monitoreo	El equipo debe ser accesible a través de SSH, cliente o a través de una interfaz Web usando SSL.				

	7. Capacidad de Almacenamiento	El equipo debe tener almacenamiento con redundancia en sus discos duros, con capacidad de al menos 2 x 2 TB (RAID1).				
	8. Redundancia de Energía	El equipo debe incluir fuentes de poder redundantes con tecnología hot swappable.				
	9. Memoria RAM	36 GB				
	10. Procesador	1 CPU, 8 Cores físicos				
	11. Formato	El equipo debe poder ser instalado en rack estándar (debe incluir los accesorios de instalación)				
	12. Dispositivo de hardware certificado	El dispositivo de hardware sobre el que deberá ejecutarse la solución de seguridad perimetral deberá estar certificado y garantizado del correcto funcionamiento del software por parte del fabricante de la solución.				
1	**Administración de la política de seguridad**	**La solución deberá contar con una herramienta tipo consola de administración para la configuración y gestión de los parámetros de las políticas de seguridad de la solución perimetral de forma centralizada.**				
	1. Acceso basado en roles	Debe soportar cuentas de administrador basadas en roles, incluyendo al menos: read/write y read only o que se puedan personalizar.				
	2. Múltiples métodos de autenticación	Debe soportar autenticación por una base de datos local, LDAP, TACACS, RADIUS o SecureID				
	3. Canal de comunicaciones seguro	Las comunicaciones entre todos los componentes que pertenezcan a un solo dominio de administración (servidor de administración, gateways) se deben establecer a través del uso de un canal de comunicaciones seguro basado en certificado para el cifrado.				

	4. Gestión Centralizada	Todas las aplicaciones de seguridad deben ser gestionados desde la consola central gráfica, donde las reglas puedan ser creadas mediante objetos.				
	5. Opción de búsqueda	La solución debe incluir una opción de búsqueda que permita consultar fácilmente que objeto de red contiene una dirección IP específica o una parte de ella.				
	6. Drag and Drop	Debe ser capaz de soportar "Drag and Drop" de objetos y deben de poder ser utilizados en varias políticas.				
	7. Segmentación de reglas de seguridad	Debe incluir la opción de segmentar las reglas de seguridad, usando etiquetas o títulos de sección y de esa forma organizar mejor la política de seguridad.				
	8. Verificación de política previo a su aplicación	Debe tener un mecanismo de verificación de la política de seguridad antes de su instalación.				
	9. Verificación previo a conflictos en reglas	La solución debe realizar una verificación de las políticas de seguridad creadas de modo que no existan conflicto de reglas				
	10. Consola centralizada con funcionalidades de monitoreo	La Administración debe ser de forma centralizada a través de una sola consola de monitoreo de políticas de Firewall, Filtrado Web, Control de Aplicaciones, Control de ancho de banda, IPS, antimalware/antispyware, anti botnets; en un solo equipo central con funcionalidades de monitoreo en tiempo real y reporteo independiente.				
	11. Contador de utilización (HITS)	Debe tener contador de utilización (HITS) en las reglas de seguridad, para saber que tanto se utilizan las reglas. Éste contador debe ser visible en la misma lista de reglas de				

		seguridad				
	12. Auditoria de cambios realizados	Seguimiento a los cambios realizados en las políticas de seguridad, de modo que sea posible revisar qué administrador hizo qué modificaciones, así como fecha, origen e impacto de la modificación.				
	13. Aplicación de actualizaciones	Debe incluir la habilidad de distribuir y aplicar centralizadamente nuevas versiones de software para los módulos de la solución.				
	14. Gestión de licencias centralizada	Debe incluir una herramienta que administre centralizadamente la licencia de todos los módulos, controlados desde la estación de administración.				
	15. Bitácoras de estado de la seguridad	Generar bitácoras, que permitan obtener fácilmente un reporte completo del estado de la seguridad de la red.				
	16. Integración con LDAP	Integración transparente y certificada con directorios tipo LDAP.				
	17. Versionamiento de policitas de seguridad	Generar versiones de la política de seguridad, y poder regresar a versiones anteriores de la misma.				
	18. Monitoreo en tiempo real	Monitoreo en tiempo real del tráfico a través de los módulos administrados, monitoreo de sesiones además de monitorear el estado de cada uno de los puntos de refuerzo que se encuentren en toda la red, en tiempo real.				
	19. Vista Global	Debe tener una vista global que permita detectar notificaciones o estado de los equipos.				
	20. Ejecución programada de scripts	Debe soportar ejecución programada de script en los equipos que permita ejecutar comandos como creación de copias de seguridad, reinicios				

		de equipo, aplicación de cambios de políticas entre otros.				
	21. Operaciones mínimas	Entre las operaciones debe incluir como mínimo cambios de tabla de ruteo, DNS, interfaces y copias de seguridad.				
	22. Ejecución de scripts remoto	Debe permitir ejecutar scripts remotamente desde la consola de administración				
	23. Modo mantenimiento	Debe poder colocar los equipos en un modo fuera de línea o mantenimiento, de modo que la configuración del sistema sea local.				
2	**Identificación de Usuarios**	**La solución deberá poder identificar plenamente y de manera centralizada el acceso, uso y utilización de usuarios a recursos y aplicaciones de internet.**				
	1. Control granular basada en usuarios	Visibilidad y control granular basada en usuarios, grupos de usuarios, máquinas.				
	2. Integración con Active Directory	Identificación de usuario integrado a Microsoft Active Directory.				
	3. Identificación mediante portal cautivo	Identificación de usuarios y máquinas externas mediante portal cautivo.				
	4. Identificación mediante agentes	Identificación de usuarios mediante agentes tanto para estaciones de trabajo como para servidores de aplicaciones como Citrix y Terminal Services.				
	5. Identificación de usuarios remotos	Identificación de los usuarios que se conectan por medio de VPN de acceso remoto, para clientes SSL VPN y IPSec VPN.				
3	**Módulo de Monitoreo**	**La consola centralizada debe incluir un Módulo de Monitoreo de políticas de regulaciones y mejores prácticas en la configuración de seguridad. Este módulo de monitoreo de cumplimiento debe ser parte integral de la consola de administración**				

		centralizada.				
	1. Acceso a recomendaciones y mejores prácticas directamente del fabricante.	Debe incluir al menos 250 recomendaciones de mejores prácticas directas del fabricante. Adicional, recomendaciones que provienen de las regulaciones.				
	2. Asesoría en tiempo real	La asesoría de las regulaciones debe aplicarse en tiempo real.				
	3. Reportes automatizados de regulaciones	Debe poder generar reportes automatizados para las regulaciones.				
	4. Verificaciones de cumplimiento	Las verificaciones de cumplimiento deben revisarse con cada cambio hecho en las políticas de seguridad.				
	5. Sección de Alertas	Debe tener una sección de alertas donde se resalten violaciones a recomendaciones o regulaciones.				
	6. Notas de recomendaciones	Todas las mejores prácticas deben incluir notas de recomendaciones que permita a los administradores obtener información sobre las acciones que se deben tomar para mitigar el incidente.				
	7. Regulaciones internacionales	Debe incluir al menos 20 regulaciones internacionales entre ellas debe incluirse al menos: ISO 27001, HIPPA, PCI DSS, NIST 800-41, SOX y FIPS 200				
	8. Monitoreo de cada modulo	Debe proveer el status de cada uno de los componentes de cada modulo (firewall, vpn, antivirus, etc.) Debe proveer por lo menos la siguiente información por cada módulo: • Sistema Operativo • Uso de Memoria • CPU				
	9. Configuración de acciones	Debe poderse configurar umbrales que generen acciones cuando éstos sean superados. Las acciones deben incluir: Log, alert, send an SNMP trap, send				

		an email y execute a user defined alert.				
	10. Graficas de Monitoreo predefinidas	Debe incluir gráficas predefinidas de monitoreo vs la evolución del tiempo, del tráfico y los contadores del sistema: • Top de reglas de seguridad • Top de usuarios P2P • Túneles de VPN • Tráfico de red Debe proveer la opción de generar gráficas personalizadas así como Top sessions.				
	11. Identificación de funcionamiento inadecuado	Debe poder reconocer funcionamientos inadecuados y problemas de conectividad entre dos puntos conectados a través de una VPN, alertar y crear logs cuando el túnel de VPN se encuentre abajo, al igual que las interfaces.				
4	**Visualizador de Eventos y Reportes**	**La solución debe incluir un módulo integrado de visualización y revisión de eventos que permita visibilidad de los productos de seguridad en tiempo real.**				
	1. Solución integrada	La solución debe estar completamente integrada a la administración.				
	2. Visualización centralizada	La solución debe visualizar, revisar y analizar eventos generados por los distintos módulos de seguridad incluidos en la solución de seguridad y dispositivos de terceros				
	3. Filtros de características de eventos	Debe permitir la creación de filtros con base en cualquier característica del evento: Funcionalidad de seguridad, IP origen, IP Destino, tipo de evento, severidad del evento, nombre del ataque, país de origen y destino.				
	4. Focalización de eventos	La aplicación debe tener mecanismos para asignar los filtros a gráficos actualizados				

		periódicamente, los cuales muestran los eventos que hacen match con dichos filtros. Esto permitirá a los operadores focalizarse en estos eventos.				
	5. Eventos de seguridad	Capacidad para reporta, revisar y correlacionar eventos de seguridad.				
	6. Reportes	Debe permitir la agrupación de eventos por cualquiera de sus características y expórtalos a PDF.				
	7. Análisis forense	Debe permitir buscar dentro de un evento y ver los detalles del evento con el fin de obtener mayor información y análisis forense.				
	8. Reportes predefinidos	La solución debe incluir reportes predefinidos por hora, día, semana y mes, incluyendo al menos: Top eventos, sources, destinos, servicios				
	9. Configuración de nuevos reportes	Debe soportar la configuración de reportes programados.				
	10. Reportes automáticos	Debe soportar compartir de forma automática los reportes a través de: e-mail, ftp, web service.				
	11. Entrega de estadísticas	Debe de ser capaz de entregar estadísticas del flujo de información, por ancho de banda, por aplicación, por conexiones, por dominios.				
	12. Extracción de información desde archivos logs	Capacidad de usar una política de consolidación para extraer los datos de los archivos log.				
	13. Portal WEB	Debe incluir un portal WEB para que otros usuarios con el perfil apropiado puedan visualizar y monitorear los eventos				
5	**Repositorio de registros y eventos de seguridad**	**La solución debe contar con una herramienta capaz de realizar análisis de registros y eventos auditoría en tiempo real de los eventos de seguridad.**				

	1. Búsqueda intuitiva	Debe ser capaz de realizar búsquedas intuitivas en la totalidad de los registros almacenados en el dispositivo.				
	2. Búsquedas granulares	Debe permitir realizar búsquedas granulares para cualquier comunicación o de patrón de tráfico.				
	3. Limitaciones	Debe ser una herramienta sin límite de registros, debe estar limitada solo por el tamaño del espacio en disco.				
	4. Reducir el tiempo de revisión de incidentes	Deberá ser posible reducir el tiempo de troubleshooting al poder mostrar resultados en tiempo real.				
	5. Filtros predefinidos para búsquedas	Debe tener filtros predefinidos de búsqueda y permitir crear y salvar filtros personalizados.				

LOTE 5: ADQUISICION E INSTALACIÓN DE UNA SOLUCION DE COMUNICACIONES TELEFONICA IP DE CLASE EMPRESARIAL PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

Actualmente IHSS cuenta con una plataforma Tecnológica tanto en infraestructura para el transporte de datos como de servicios sistematizados.

Bajo este concepto el IHSS está avanzando en los cambios tecnológicos y que estén a la vanguardia de los requerimientos institucionales actuales, por lo que a través de este proyecto se desea adquirir, implementar y desarrollar una solución de comunicaciones de Telefonía IP o VoIP que pueda ser integrada a la infraestructura de redes y conectividad actualmente instalada y que sea capaz de cumplir las diversas necesidades de transmitir voz, datos, imágenes y video de forma simultánea, parte de este proceso es trabajar en una solución integral que sea abierta, escalable, estable, segura y confiable que permita incorporar o implementar un servicio digital denominado DID (Direct Inward Dialling) para todas las localidades del IHSS a nivel nacional.

Dicho servicio permitirá tener mayores facilidades en el uso de la Telefonía IP como ser, mayor cantidad de números telefónicos en un solo troncal y con escalabilidad, contrario a las líneas telefónicas análogas existentes en el Instituto.

Otra facilidad es la calidad en el servicio de voz (QoS) ya que la línea digital o DID está libre de ruido y a esto se suma la reducción de los costos que se tendrán a mediano plazo.

La propuesta debe incluir:

Equipo de telefonía IP de clase empresarial que incluya lo siguiente:

- 3 equipos de comunicaciones de telefonía IP (dispositivo, softwares y servicios), incluyendo componentes y accesorios necesarios para su puesta en producción.
- Componente de administración y monitoreo (dispositivo, softwares y servicios); incluyendo componentes y accesorios necesarios para su puesta en producción.
- Servicios de Instalación configuración y pruebas de la solución de infraestructura, equipos, componentes y su software de gestión.
- Verificación del correcto funcionamiento de la solución de infraestructura, equipos, componentes y su software de gestión.
- Servicios de capacitación por parte del representante del fabricante o representante en el uso, administración, configuración y monitoreo de la solución adquirida para el Área de Infraestructura de la Gerencia de IT del IHSS, para ocho personas un mínimo.
- Servicio de garantía del fabricante: los equipos, todos sus componentes de hardware y software deben de tener una garantía 1 año como mínimo.
- Soporte técnico (local y remoto cuando fuera necesario), actualizaciones y corrección de errores.
- El proveedor deberá incluir todos los accesorios, medios, equipos, etc que sean necesarios para la instalación y puesta en producción del equipo.
- La empresa deberá entregar nota del fabricante de la solución donde se indique que esta cuenta con la capacidad técnica y el respaldo de la marca y del fabricante para el tipo de implementación de productos y servicios descritos en el LOTE 5: ADQUISICION E

Descripción General

El IHSS pretende adquirir, implementar y desarrollar una solución de comunicaciones de Telefonía IP o VoIP de última generación y de clase empresarial, mediante el uso de herramientas de hardware y software para la implementación de servicios de valor añadido en un ambiente avanzado de telefonía y servicios multimedia en general. El sistema de comunicación telefónica IP que se debe proponer debe de nivel empresarial, flexible, escalable y de última generación.

La solución deberá contar con funcionalidades comunicación de alta tecnología que garantice efectividad, disponibilidad y un buen servicio de atención al IHSS.

Alcance de la oferta

- Instalar e implementar un sistema de comunicación telefónica IP (**3 dispositivos PBX**) que se integren a la Plataforma Tecnológica actual del IHSS y permita cubrir las necesidades de transmitir voz y datos, que demanda el IHSS y sus 32 localidades remotas a nivel nacional, mediante su actual infraestructura de las redes LAN y WAN.
- Instalación y configuración de los dispositivos (Appliances).

Se requieren la adquisición de **3 dispositivos centrales de telefonía IP** los cuales estarán ubicados físicamente en los siguientes sitios:

1. Edificio Administrativo del IHSS, Barrio Abajo, Tegucigalpa
2. Hospital de Especialidades, Barrio La Granja, Comayagüela
3. Hospital Regional del Norte, San Pedro Sula, Cortes

Para toda la implementación deberán ser incluidos los suministros de materiales, accesorios y componentes necesarios para la instalación de la solución.

Pruebas de funcionamiento de los equipos y la aplicación en cada sitio. Los resultados que se desean alcanzar son:

- Comunicación unificada.
- Administración y resolución de errores.
- Reducción de costos en el consumo de llamadas.
- Crear un ámbito efectivo de respuesta a solicitudes de los usuarios.
- Call Center.
- Efectividad y seguridad.

REQUERIMIENTOS

Factibilidad Técnica.

A continuación, se enumeran los siguientes aspectos técnicos con lo que ya cuenta el IHSS:

- Redes LAN en cada una de las localidades, con cableado categoría 5e y fibra óptica en algunos casos; con switches de conectividad capa 2 y capa 3.
- Red WAN a nivel nacional, conectadas a través de un ISP.
- Centro de datos en los tres sitios principales a donde se deberán instalar los appliances o dispositivos centrales. Los centros de datos poseen las características propias de un Data Center como ser aire acondicionado de precisión, UPS centralizado con alta capacidad en baterías de respaldo, etc.

Diseño

Para la implementación del proyecto se desee instalar 3 dispositivos (appliances) centrales, en:

1. Edificio Administrativo del IHSS, Barrio Abajo, Tegucigalpa
2. Hospital de Especialidades, Barrio La Granja, Comayagüela
3. Hospital Regional del Norte, San Pedro Sula, Cortes

Se requiere que los dispositivos sean para instalación en rack, la solución deberá ser integral, es decir, ser de un único fabricante en sus componentes los cuales formaran un diseño integrado y garantizado, tanto en hardware como en software, con disponibilidad en fuentes de poder y ventiladoras internas.

La señalización que recibirá el IHSS será tipo E1 (líneas digitales) en forma posterior y ajena a este proceso, según la distribución del proveedor de acuerdo a la siguiente tabla:

SITIO	TIPO DE CONEXIÓN	LLAMADAS SIMULTANEAS
Edificio Administrativo TGU	2 canales E1	60
Hospital de Especialidades Comayagüela	2 canales E1	60
Hospital Regional del Norte, San Pedro Sula	2 canales E1	60

Los dispositivos de la solución telefónica deberán estar interconectados a través de las redes LAN/WAN del IHSS.

Distribución de Extensiones

Como fase inicial y para escalabilidad futura según los requerimientos se pretende iniciar con una cantidad estimada de extensiones de acuerdo a la siguiente tabla:

SITIOS		Líneas Telefónicas
1	Campus del Edificio Administrativo IHSS Barrio Abajo	
	Edificio Administrativo	220
	Clínica Periférica 1 (Campus Barrio Abajo)	90
	Edificio Adulto Mayor	25
	Edificio IVM	24
	Edificio Capacitaciones	3
2	Hospital de Especialidades, Tegucigalpa	150
3	Almacén Central, Tegucigalpa	5
4	Periférica 3 Kennedy, Tegucigalpa	10
5	Periférica 2 Santa Fe, Tegucigalpa	10
6	Centro de Rehabilitación Pediátrica, Colonia El Prado, Tegucigalpa	3
7	Regional Choluteca, Choluteca	3
8	Regional y Clinica de Danlí El Paraíso	3
9	Regional El Paraíso, El Paraíso	3
10	Regional San Lorenzo (Jícaro), Valle	3
11	Regional Catacamas, Olancho	3
12	Regional Juticalpa, Olancho	3
14	Regional Comayagua, Comayagua	3
15	Regional Siguatepeque, Comayagua	3
16	Clínica Regional de Choluteca, Choluteca	3
17	Clínica de Monjarás, Choluteca	3
18	Hospital Regional del Norte, San Pedro Sula	150
19	Regional Orquídea Blanca, San Pedro Sula	10
20	Clínica 1:Tepeaca, San Pedro Sula	10
21	Clínica 2: Calpules, San Pedro Sula	10
22	Regional Villanueva, Cortés	10
23	Regional Choloma, Cortés	10
24	Clínica Puerto Cortés, Cortés	3
25	Clínica El Progreso, Yoro	10
26	Regional Tocoa, Colón	5
27	Regional Islas de la Bahía, Roatán	3
28	Regional Santa Rosa de Copán, Copán	3
29	Clínica La Ceiba, Atlántida	10
30	Regional La Ceiba, Atlántida	10
31	Regional Tela, Atlántida	3

32	Regional Naco, Cortés	3
33	Regional Olanchito, Yoro	3
	TOTAL LINEAS TELEFONICAS	**826**

Actualmente la red WAN del IHSS es operada por medio de canales de datos que interconectan a las localidades remotas con el Edificio Administrativo en Tegucigalpa.

Los medios utilizados por la empresa ISP son enlaces de fibra óptica, con un ancho de banda en promedio de 100 Mbps para las clínicas y oficinas regionales, y 1 Gbps entre los sitios principales como ser Edificio Administrativo en Tegucigalpa, Hospital de Especialidades en Comayagüela y Hospital Regional del Norte en San Pedro Sula.

La autenticación de las extensiones de la zona centro sur (a excepción del Hospital de Especialidades) se deberán realizar en el dispositivo ubicado en el Edificio Administrativo; y la zona nor occidental en el dispositivo en el Hospital Regional del Norte.

ESPECIFICACIONES TECNICAS DE EQUIPOS

Se requiere adquirir e implementar una solución que deberá disponer, de forma general, de las máximas funcionalidades en red permitidas por la tecnología actual, debiendo garantizarse siempre la actualización progresiva de las mismas, en función de la evolución tecnológica.

A continuación, se enumeran las características que deberán cumplir los equipos para telefonía a implementar.

Especificaciones técnicas del Appliance o central de comunicaciones unificadas

Cantidad: 3

El appliance propuesto deberá integrar en forma obligatoria la telefonía analógica, digital (DID) y móvil, deberán salir a través de los appliances utilizando números cortos para las extensiones y para las llamadas externas de forma directa, a excepción para las llamadas a móviles.

También debe cumplir otras características como:

1. Grabación de Llamadas.
2. Correo de Voz.
3. IVR Configurable y Flexible para cada PBX.
4. Soporte para Sintetización de Voz.
5. Herramienta para la creación de extensiones por lote.
6. Cancelador de eco integrado.
7. Provisionador de Teléfonos vía Web.
8. Soporte para videófonos.
9. Interfaz de detección de Hardware.
10. Servidor DHCP para asignación dinámica de IP´s.
11. Panel de Operador basado en Web.
12. Llamadas en espera.

13. Reporte de detalle de llamadas (CDR).
14. Tarificación con reporte de consumo por destino.
15. Reportes de uso de canales.
16. Soporte para colas de llamadas.
17. Centro de Conferencias con Salas Virtuales.
18. Soporte para protocolos SIP e IAX, entre otros.
19. Codecs Estandares de la industria
20. Soporte para interfaces digitales E1/T1/J1 a través de los protocolos PRI/BRI/R2.
21. Identificación de llamadas (Caller ID) para las líneas digitales
22. Rutas entrantes y salientes con configuración por coincidencia de patrones de marcado.
23. Soporte para follow-me.
24. Soporte para grupos de timbrado.
25. Soporte para paging e intercom.
26. Soporte para condiciones de tiempo.
27. Soporte para PINes de seguridad.
28. Soporte para DISA (Direct Inward System Access).
29. Soporte para Callback.

El equipo ofertado debe permitir la creación de PBX virtuales como **mínimo** para:

1. Emergencias Tegucigalpa (PBX para el área de emergencias del Hospital de Especialidades)
2. Emergencias San Pedro Sula (PBX para el área de emergencias del Hospital Regional del Norte)
3. Edificio Administrativo (Barrio Abajo)
4. Periférica Numero 1, 2 y 3, Clínica de Adulto Mayor
5. Edificio IVM
6. Almacén Central
7. Hospital de Especialidades
8. Hospital Regional del Norte
9. Periférica Calpules y Tepeaca, Villanueva

Características del Módulo Call Center

El IHSS desea establecer una central de llamadas (call center) que permita realizar o recibir llamadas para atender las necesidades y dar un servicio u orientación al usuario.

Se debe ofertar un sistema amigable que permita al personal de call center manejarlo con facilidad. Debe cumplir otras características como:

1. Administración web
2. Soporte para Do-Not-Call List
3. Soporte para generación y configuración de breaks
4. Soporte para integración de aplicaciones externas (CRM, Formularios) en campaña
5. Soporte para diseño de formularios
6. Soporte para la generación de guión por campañas y por colas
7. Almacenamiento de guión de atención
8. Soporte para reintentos en campañas salientes

9. Soporte para exportación de reportes a hojas de cálculo, PDF y CSV
10. Consola de agente basada en web Soporte de transferencia de llamada desde consola
11. Capacidad de colocar una llamada en espera
12. Soporte para campañas entrantes y salientes
13. Soporte para agendamiento de llamada en campañas salientes
14. Soporte para agendamiento de llamada asignada al mismo agente
15. Soporte para call back login
16. Ejecución de múltiples campañas simultáneas.
17. Seguimiento de agente asignado a una llamada.
18. Soporte para grabación de llamadas por colas
19. Marcador predictivo
20. Soporte para configuración de umbral de llamada corta
21. Configuración de espera máxima de llamada marcada
22. Soporte para activación/desactivación de predicción
23. Llamado automático a partir de un listado de números
24. Asignación de eventos asincrónicos al agente

CARACTERISTICAS DE LOS TELEFONOS

Tipos de Teléfonos IP

El IHSS implementará una solución de telefonía IP por lo que requerirá los equipos telefónicos IPs a los usuarios y para efectos de esta oferta el IHSS desea adquirir teléfonos IP´s para cumplir con la demanda que la solución propondrá y serán en base inicial a la siguiente tabla:

Tipo	Categoría	Cantidad
1	Semi-Ejecutivo	43
2	Básico	767
3	Operador (vía software o softphone)	10
4	Conferencia	6
	Total	**826**

La solución también deberá tener la posibilidad de hacer la instalación de cliente softphone, es decir que sea instalable en un equipo PC estándar.

Tipo 1 (Semi Ejecutivo)

1. Soporte para protocolo de señalización SIP, SIP v2
2. Pantalla gráfica: Visualización en pantalla de textos y gráficos(Monocromática)
3. Características telefónicas tradicionales: tales como re discado de llamadas, transferencia de llamadas y conferencias de audio al menos tres interlocutores. Se valorará la posibilidad de hacer Pickup Group o Direct Pickup.
4. Registración automática o con pre-configuración mínima (Usuario, PIN y línea) en el sistema telefónico al conectarse a la red corporativa.
5. Comunicaciones integradas, manejo de voz y datos.

6. Switch Ethernet: Conexiones 10/100 BASE-T o 10/100/1000 BASE-T con conectores RJ45, uno para la conexión LAN y el otro para la conexión de un PC u otro dispositivo de red en cascada.
7. Direccionamiento a través de cliente DHCP.
8. Funcionalidad de llamada en espera (funcionalidad obligatoria incluyendo música durante el estado de Holding opcional).
9. Compatibilidad con IEEE 802.3af Power over Ethernet. (Se deberá incluir la Fuente de poder independiente del equipo)
10. Control de volumen.
11. Soporte de lenguaje: Español.
12. Acceso directo a voicemail.
13. Multi línea (opcional)
14. Indicadores de estado de línea luminosos. (opcional).
15. Capacidad de manejo de agenda de contactos.
16. Soporte de protocoles de audio G711 y G729 (mínimo)
17. Funcionalidad de Manos libres full duplex.
18. Conector para vincha.
19. Soporte aplicaciones XML(opcional)
20. Soporte up grade de software usando TFTP.
21. Detección de voz (VAD), supresión de silencios, y “Confort noise “.

Tipo 2 (Básico)

1. Soporte para protocolo de señalización SIP
2. Pantalla:
    a. Visualización de textos y gráficos.
    b. Monocromática.
3. Funcionalidad de consola de atención.
4. Botones iluminados con señalización de estado de línea por colores.
5. Botones de consola programables como:
    a. Números de directorio telefónico
    b. Indicadores de estado de línea.
    c. Discado rápido
6. Características telefónicas tradicionales: tales como re discado de llamadas, transferencia de llamadas y conferencias de audio al menos tres interlocutores. Se valorará la posibilidad de hacer Pickup Group o Direct Pickup.
7. Registración automática o con pre configuración mínima (Usuario, PIN y línea) en el sistema telefónico al conectarse a la red corporativa.
8. Comunicaciones integradas, manejo de voz y datos.
9. Switch Ethernet: Conexiones 10/100 BASE-T o 10/100/1000 BASE-T con conectores RJ45, uno para la conexión LAN y el otro para la conexión de un PC u otro dispositivo de red en cascada.
10. Direccionamiento a través de cliente DHCP.
11. Funcionalidad de llamada en espera obligatoria. Música durante el estado de Holding opcional.
12. Compatibilidad con IEEE 802.3af Power over Ethernet. (Se deberá incluir la Fuente de poder independiente del equipo)

13. Control de volumen.
14. Soporte de lenguaje: Español.
15. Acceso directo a voicemail.
16. Multi línea (al menos 12 líneas)
17. Indicadores de estado de línea luminosos. (opcional)
18. Capacidad de manejo de agenda de contactos.
19. Soporte de protocoles de audio G711 y G729 (mínimo)
20. Funcionalidad de Manos libres full duplex.
21. Conector para vincha.
22. Soporte aplicaciones XML Soporte up grade de software usando TFTP.
23. Detección de voz (VAD), supresión de silencios, y “Confort noise.

Tipo 3 (Operadora, vía software o softphone)

1. Las mismas incluirán el DSP y se conectarán por USB, como forma de garantizar su buena calidad de sonido
2. Vincha con Auricular y Mic.
3. Control de Volumen y Mute
4. De uso intensivo y calidad empresarial.

Se deberán incluir los componentes necesarios para la instalación en los equipos PCs necesarios, tarjetas, diademas, drivers, software, licencias, accesorios, etc.

El IHSS proveerá los equipos (diez) PCs estándar, en caso de que se requiera un equipo especializado, el oferente deberá indicarlo y proponerlo.

Tipo 4 (Teléfono para Conferencias)

1. Soporte para protocolo/normas estándares de la industria
2. Puerto ethernet con detección automática (100/1000 Mbps) y PoE integrado
3. Pantalla Grafica
4. Micrófono con captación de al menos 12 pies de distancia
5. Altavoz con volumen al menos 86 dB a 0.5 metros de distancia
6. Conectividad WiFi integrada
7. Puertos auxiliares de audio de 3.5 mm, Micro USB
8. Funciones de telefonía: al menos Retención, transferencia, desvío, conferencia de 7 vías, captura de llamadas, llamada en espera.
9. Debe contar con alta calidad de audio
10. Capacidad para QoS
11. Contraseñas a nivel de usuario y administrador.
12. Multilenguaje, debe incluir al menos el idioma español e inglés.
13. Incluir los accesorios necesarios para su conectividad, fuente de alimentación, cables de red, etc.

OTRAS CONDICIONES TÉCNICAS OBLIGATORIAS

1. Ofrecer un servicio de Soporte Técnico o Help Desk de solución de problemas básicos y/o inicio de procedimiento de Soporte avanzado (mínimo 5 días por 9 horas). Este servicio debe ser suministrado a la Gerencia de Tecnologías de Información y Comunicaciones del IHSS, con un óptimo nivel de calidad y la forma en que se prestará, deberá estar detallada en la propuesta.
2. Se debe garantizar soporte técnico de calidad, durante el periodo de la garantía con sistemas de atención y de comunicaciones que faciliten el servicio, tales como conmutadores, líneas de servicio al cliente y/o soporte en línea.
3. Dentro del tiempo de garantía el proponente hará la reposición de los equipos o del cambio de las partes en caso de presentarse alguna falla, por partes nuevas de iguales o superiores características en los lugares en que se instalen los equipos.
4. En caso de que un repuesto no se encuentre en las instalaciones de la empresa tendrá un plazo de máximo de VEINTE (20) días calendario para remplazarlo.
5. En la oferta se deberá contemplar un acompañamiento de instalación y configuración de los equipos junto con el personal técnico de la Gerencia de Tecnologías de Información y Comunicaciones.
6. Ocho personas deberán ser capacitadas para el uso, administración y gestión de la solución de telefonía IP.

ET-03 ACCESORIOS

Detalle de los accesorios que deben acompañar necesariamente al suministro principal ***(ver especificaciones) (No Aplica)***

ET-04 SERIES

ET-05

CATÁLOGO

Se requiere obligatoriamente que para uno de los equipos y componentes se presente literatura descriptiva o catálogos en idioma español para cada uno de los lotes ofertados.

ET-06 OTROS

ALCANCE Y ESPECIFICACIONES TECNICAS

Justificación:

El IHSS realizo la adquisición e instalación de equipos de comunicaciones para los edificios principales a mediados de 2005 y durante el año 2011; actualmente mucha de esta infraestructura de redes se encuentra con fallas y falencias técnicas. Estos equipos concentran las conexiones de fibra óptica (el cual también se encuentra con deficiencias físicas) y las conexiones de cableado estructurado de cobre entre los equipos clientes; como ser servidores, computadoras de escritorios, equipo portátil, equipos de comunicaciones de acceso y las comunican con los servidores de aplicaciones y de servicios locales en dichos sitios; y a su vez conectan los equipos con las aplicaciones, bases de datos y demás

servicios en el centro de datos principal del IHSS en Barrio Abajo.
Los equipos que actualmente se encuentran en funcionamiento están obsoletos ya que fueron instalados y puestos en producción desde el año 2005, algunos componentes presentan daños físicos debido a su funcionamiento interrumpido y ya no están soportados por el fabricante, con altas probabilidades de daños completos y que el fabricante no podrá solucionar por no estar soportados, ni contar con repuestos en el mercado.
Debido a que las operaciones de atención al derechohabiente, consulta médica, hospitalización, farmacias, exámenes de laboratorios y demás servicios que se prestan a la administración a través de los sistemas financieros contables del IHSS en estos sitios, así como las conexión a servicios de Internet, correo electrónico, etc.; son de alta prioridad para la continuidad del negocio del IHSS y están soportados bajo estas soluciones de comunicaciones y protección de la red interna/perimetral en la totalidad de la red LAN/WAN del IHSS; es de importante necesidad el reemplazo de los equipos que actualmente se encuentran en producción debido a la alta probabilidad de falla y a las deficiencias en la seguridad de la red institucional del IHSS.

ALCANCE:
Los alcances del proveer para estas implementaciones son:

- Aprovisionamiento del equipo, accesorios, componentes.
- Instalación, implementación, pruebas y puesta en producción de todas las soluciones descritas en este documento de licitación.
- Garantía del fabricante.
- Soporte técnico post implementación.
- Accesorios, el oferente deberá contemplar para la puesta en marcha de la solución al menos lo siguiente: Las accesorios, componentes y software necesarios para la realización de instalación de equipos, Los cables de conexión eléctrica AC
- Documentación del equipo en físico o electrónico.
- Capacitación, se deberá brindar capacitación técnica en el uso de la totalidad de la solución descrita en estas bases de licitación.

Formulario de Presentación de la Oferta

[El Oferente completará este formulario de acuerdo con las instrucciones indicadas. No se permitirán alteraciones a este formulario ni se aceptarán substituciones.]

Fecha: *[Indicar la fecha (día, mes y año) de la presentación de la Oferta]*
LPN No.*: [indicar el número del proceso licitatorio]*

A: *[nombre completo y dirección del Comprador]*

Nosotros, los suscritos, declaramos que:

(a) Hemos examinado y no hallamos objeción alguna a los documentos de licitación, incluso sus Enmiendas Nos. *[indicar el número y la fecha de emisión de cada Enmienda];*

(b) Ofrecemos proveer los siguientes Bienes y Servicios de conformidad con los Documentos de Licitación y de acuerdo con el Plan de Entregas establecido en la Lista de Requerimientos: *[indicar una descripción breve de los bienes y servicios];*

(c) El precio total de nuestra Oferta, excluyendo cualquier descuento ofrecido en el rubro (d) a continuación es: *[indicar el precio total de la oferta en palabras y en cifras, indicando las diferentes cifras en las monedas respectivas];*

(d) Los descuentos ofrecidos y la metodología para su aplicación son:

Descuentos. Si nuestra oferta es aceptada, los siguientes descuentos serán aplicables: *[detallar cada descuento ofrecido y el artículo específico en la Lista de Bienes al que aplica el descuento]*.

Metodología y Aplicación de los Descuentos. Los descuentos se aplicarán de acuerdo a la siguiente metodología: *[Detallar la metodología que se aplicará a los descuentos];*

(e) Nuestra oferta se mantendrá vigente por el período establecido en la Sub cláusula 20.1 de las IAO, a partir de la fecha límite fijada para la presentación de las ofertas de conformidad con la Sub cláusula 24.1 de las IAO. Esta oferta nos obligará y podrá ser aceptada en cualquier momento antes de la expiración de dicho período;

(f) Si nuestra oferta es aceptada, nos comprometemos a obtener una Garantía de Cumplimiento del Contrato de conformidad con la Cláusula 44 de las IAO y Cláusula 17 de las CGC;

(g) La nacionalidad del oferente es: [indicar la nacionalidad del Oferente, incluso la de todos los miembros que comprende el Oferente, si el Oferente es un Consorcio]

(h) No tenemos conflicto de intereses de conformidad con la Cláusula 4 de las IAO;

(i) Nuestra empresa, sus afiliados o subsidiarias, incluyendo todos los subcontratistas o proveedores para ejecutar cualquier parte del contrato son elegibles, de conformidad con la Cláusula 4 de las IAO;

(j) Las siguientes comisiones, gratificaciones u honorarios han sido pagados o serán pagados en relación con el proceso de esta licitación o ejecución del Contrato: [indicar el nombre completo de cada receptor, su dirección completa, la razón por la cual se pagó cada comisión o gratificación y la cantidad y moneda de cada dicha comisión o gratificación]

Nombre del Receptor	Dirección	Concepto	Monto

(Si no han sido pagadas o no serán pagadas, indicar "ninguna".)

(k) Entendemos que esta oferta, junto con su debida aceptación por escrito incluida en la notificación de adjudicación, constituirán una obligación contractual entre nosotros, hasta que el Contrato formal haya sido perfeccionado por las partes.

(l) Entendemos que ustedes no están obligados a aceptar la oferta evaluada como la más baja ni ninguna otra oferta que reciban.

Firma: *[indicar el nombre completo de la persona cuyo nombre y calidad se indican]* En calidad de *[indicar la calidad jurídica de la persona que firma el Formulario de la Oferta]*

Nombre: *[indicar el nombre completo de la persona que firma el Formulario de la Oferta]*

Debidamente autorizado para firmar la oferta por y en nombre de: [*indicar el nombre completo del Oferente]*

El día_____del mes_____del año_____*[indicar la fecha de la firma]*

Declaración Jurada sobre Prohibiciones o Inhabilidades

Yo_____, mayor de edad, de estado civil_____, de nacionalidad_____, con domicilio en _____ _____y con Tarjeta de Identidad/pasaporte No._____actuando en mi condición de representante legal de ____(Indicar el Nombre de la Empresa Oferente / En caso de Consorcio indicar al Consorcio y a las empresas que lo integran)_____ _____, por la presente HAGO DECLARACIÓN JURADA: Que ni mi persona ni mi representada se encuentran comprendidos en ninguna de las prohibiciones o inhabilidades a que se refieren los artículos 15 y 16 de la Ley de Contratación del Estado, que a continuación se transcriben:

"ARTÍCULO 15.- Aptitud para contratar e inhabilidades. Podrán contratar con la Administración, las personas naturales o jurídicas, hondureñas o extranjeras, que, teniendo plena capacidad de ejercicio, acrediten su solvencia económica y financiera y su idoneidad técnica y profesional y no se hallen comprendidas en algunas de las circunstancias siguientes:
1) Haber sido condenados mediante sentencia firme por delitos contra la propiedad, delitos contra la fe pública, cohecho, enriquecimiento ilícito, negociaciones incompatibles con el ejercicio de funciones públicas, malversación de caudales públicos o contrabando y defraudación fiscal, mientras subsista la condena. Esta prohibición también es aplicable a las sociedades mercantiles u otras personas jurídicas cuyos administradores o representantes se encuentran en situaciones similares por actuaciones a nombre o en beneficio de las mismas;
2) DEROGADO;
3) Haber sido declarado en quiebra o en concurso de acreedores, mientras no fueren rehabilitados;
4) Ser funcionarios o empleados, con o sin remuneración, al servicio de los Poderes del Estado o de cualquier institución descentralizada, municipalidad u organismo que se financie con fondos públicos, sin perjuicio de lo previsto en el Artículo 258 de la Constitución de la República;
5) Haber dado lugar, por causa de la que hubiere sido declarado culpable, a la resolución firme de cualquier contrato celebrado con la Administración o a la suspensión temporal en el Registro de Proveedores y Contratistas en tanto dure la sanción. En el primer caso, la prohibición de contratar tendrá una duración de dos (2) años, excepto en aquellos casos en que haya sido objeto de resolución en sus contratos en dos ocasiones, en cuyo caso la prohibición de contratar será definitiva;

6) Ser cónyuge, persona vinculada por unión de hecho o parientes dentro del cuarto grado de consanguinidad o segundo de afinidad de cualquiera de los funcionarios o empleados bajo cuya responsabilidad esté la precalificación de las empresas, la evaluación de las propuestas, la adjudicación o la firma del contrato;
7) Tratarse de sociedades mercantiles en cuyo capital social participen funcionarios o empleados públicos que tuvieren influencia por razón de sus cargos o participaren directa o indirectamente en cualquier etapa de los procedimientos de selección de contratistas. Esta prohibición se aplica también a las compañías que cuenten con socios que sean cónyuges, personas vinculadas por unión de hecho o parientes dentro del cuarto grado de consanguinidad o segundo de afinidad de los funcionarios o empleados a que se refiere el numeral anterior, o aquellas en las que desempeñen, puestos de dirección o de representación personas con esos mismos grados de relación o de parentesco; y,
8) Haber intervenido directamente o como asesores en cualquier etapa de los procedimientos de contratación o haber participado en la preparación de las especificaciones, planos, diseños o términos de referencia, excepto en actividades de supervisión de construcción.

ARTÍCULO 16.- Funcionarios cubiertos por la inhabilidad. Para los fines del numeral 7) del Artículo anterior, se incluyen el Presidente de la República y los Designados a la Presidencia, los Secretarios y Subsecretarios de Estado, los Directores Generales o Funcionarios de igual rango de las Secretarías de Estado, los Diputados al Congreso Nacional, los Magistrados de la Corte Suprema de Justicia, los miembros del Tribunal Supremo Electoral, el Procurador y Subprocurador General de la República, los magistrados del Tribunal Superior de Cuentas, el Director y Subdirector General Probidad Administrativa, el Comisionado Nacional de Protección de los Derechos Humanos, el Fiscal General de la República y el Fiscal Adjunto, los mandos superiores de las Fuerzas Armadas, los Gerentes y Subgerentes o funcionarios de similares rangos de las instituciones descentralizadas del Estado, los Alcaldes y Regidores Municipales en el ámbito de la contratación de cada Municipalidad y los demás funcionarios o empleados públicos que por razón de sus cargos intervienen directa o indirectamente en los procedimientos de contratación."

En fe de lo cual firmo la presente en la ciudad de _____, Departamento de _____, a los _____ días de mes de _____de_____.

Firma: _____

Esta Declaración Jurada debe presentarse en original con la firma autenticada ante Notario (En caso de autenticarse por Notario Extranjero debe ser apostillado).

Formularios de Listas de Precios

[El Oferente completará estos formularios de Listas de Precios de acuerdo con las instrucciones indicadas. La lista de servicios en la columna 1 de la Lista de Precios deberá coincidir con la Lista de Bienes y Servicios detallada por el Comprador en los Requisitos de los Bienes y Servicios.]

Lista de Precios

LOTE	DESCRIPCION	PRECIO UNITARIO	PRECIO TOTAL
1	**ADQUISICION DE EQUIPO DE COMUNICACIONES SWITCH CORE PARA EL CENTRO DE DATOS DEL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL**		
	Equipo de comunicaciones integrado que incluye:		
	a) Componente de comunicaciones modular de clase empresarial tipo switch CORE		
	b) Componente de seguridad interna (NGFW).		
	c) Componente de administración y monitoreo		
	Servicio de Instalación, configuración, pruebas, verificación del correcto funcionamiento de la solución de infraestructura, equipos, componentes y su software de gestión, incluyendo los Accesorios, patchcords, medios, equipos, software, etc que sean necesarios para la instalación y puesta en producción del equipo.		
	Servicio de Capacitación por parte del representante del fabricante en el uso, administración, configuración y monitoreo de la solución adquirida para el Área de Infraestructura de la Gerencia de IT del IHSS, para ocho personas un mínimo		
	Servicio de Soporte Técnico por un año para toda la solución		
	Servicios de Suscripción con el fabricante por un año: el equipo deberá contar con una suscripción para descarga de archivos de definiciones de manera automática para todos los componentes de la solución, la cual deberá incluir soporte técnico (local y remoto cuando fuera necesario), actualizaciones y corrección de errores		

	TOTAL LOTE 1 (Componentes, Servicios y Accesorios)		
2	**EQUIPOS SWITCHES DE ACCESO PARA LA RED LAN DEL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL**		
	Equipos		
	Servicios de instalación y configuración		
	Servicio de Soporte Técnico por un año		
	TOTAL LOTE 2 (Componentes, Servicios y Accesorios)		
3	**CERTIFICACION Y REPARACION DE CABLEADO DE FIBRA OPTICA (BACKBONE) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL**		
	Suministro de patchcords de fibra óptica		
	Diagnóstico de los enlaces de fibra óptica que incluya la validación de capacidades de cada línea y la limpieza de gabinetes, conectores y adaptadores actualmente instalados.		
	Servicio de Reparación de fibra óptica		
	Servicio de Certificación de fibra óptica		
	TOTAL LOTE 3 (Insumos, Servicios y Accesorios)		
4	**SOLUCION DE FIREWALL DE SEGURIDAD PERIMETRAL DE PROXIMA GENERACION PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL**		
	Equipo de seguridad perimetral integrado que incluye:		
	a) Componente de seguridad perimetral		
	b) Componente de Administración y monitoreo		
	Servicio de Instalación, configuración, pruebas, verificación del correcto funcionamiento de la solución de infraestructura, equipos, componentes y su software de gestión, incluyendo los accesorios, medios, equipos, etc que sean necesarios para la instalación y puesta en producción del equipo.		

	Servicio de Capacitación por parte del representante del fabricante en el uso, administración, configuración y monitoreo de la solución adquirida para el Área de Infraestructura de la Gerencia de IT del IHSS, para seis personas un mínimo.		
	Servicios de Suscripción con el fabricante por un año: el equipo deberá contar con una suscripción para descarga de archivos de definiciones de manera automática para todos los componentes de la solución, la cual deberá incluir soporte técnico (local y remoto cuando fuera necesario), actualizaciones y corrección de errores.		
	TOTAL LOTE 4 (Componentes, Servicios y Accesorios)		
5	**ADQUISICION E INSTALACIÓN DE UNA SOLUCION DE COMUNICACIONES TELEFONICA IP DE CLASE EMPRESARIAL PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL**		
	3 equipos de comunicación telefónica IP, que incluye:		
	a) Componente de Comunicaciones de Telefonía IP		
	b) Componente de administración y monitoreo		
	Servicio de Instalación, configuración, pruebas, verificación del correcto funcionamiento de la solución de infraestructura, equipos, componentes y su software de gestión; incluyendo todos los accesorios, medios, equipos, etc que sean necesarios para la puesta en producción del equipo.		
	Servicio de Capacitación por parte del representante del fabricante o representante en el uso, administración, configuración y monitoreo de la solución adquirida para el Área de Infraestructura de la Gerencia de IT del IHSS, para ocho personas un mínimo.		
	Servicio de Soporte técnico (local y remoto cuando fuera necesario), actualizaciones y corrección de errores.		
	TOTAL LOTE 5 (Componentes, Servicios y Accesorios)		
	GRAN TOTAL		

Nombre del Oferente *[indicar el nombre completo del Oferente]* Firma del Oferente *[firma de la persona que firma la Oferta]* Fecha *[Indicar Fecha]*

Este listado de precios debe estar firmado y sellado en cada una de las páginas por el representante legal del ofertante, en papel membretado.

Los precios deberán presentarse en Lempiras y únicamente con dos decimales.

El valor total de la oferta no deberá comprender el impuesto sobre ventas, ya que **El IHSS ESTA EXENTO DE PAGO DE IMPUESTOS, según Resolución Nº DGCFA-ISV-0002-2018**.

En los cuadros de Especificaciones Técnicas para los 5 lotes el proveedor deberá indicar los folios de cumplimiento para cada especificación.

La forma de pago para uno de los ítems por lotes descritos, será de conformidad a lo establecido en CC-08 FORMA DE PAGO

FORMULARIO DE GARANTIA MANTENIMIENTO DE OFERTA NOMBRE DE ASEGURADORA / BANCO

GARANTIA / FIANZA DE MANTENIMIENTO DE OFERTA N° _____

FECHA DE EMISION: _____

AFIANZADO/GARANTIZADO: _____

DIRECCION Y TELEFONO: _____

Fianza / Garantía a favor de _____, para garantizar que el Afianzado/Garantizado, mantendrá la **OFERTA**, presentada en la licitación _____ para la prestación del Servicio "_____.

SUMA AFIANZADA/GARANTIZADA: _____

VIGENCIA De: _____ **Hasta:** _____

BENEFICIARIO: _____

Todas las garantías deberán incluir **textualmente** la siguiente cláusula obligatoria.

"LA PRESENTE GARANTÍA ES SOLIDARIA, INCONDICIONAL, IRREVOCABLE Y DE REALIZACIÓN AUTOMÁTICA, DEBIENDO SER EJECUTADA POR EL VALOR TOTAL DE LA MISMA, AL SIMPLE REQUERIMIENTO DEL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL (IHSS), ACOMPAÑADA DE LA RESOLUCIÓN ADMINISTRATIVA CORRESPONDIENTE, SIN NECESIDAD DE TRÁMITES PREVIOS AL MISMO. SIN PERJUICIO DE LOS AJUSTES QUE PUDIERAN HABER, SI FUERE EL CASO, QUE SE HARAN CON POSTERIORIDAD A LA ENTREGA DEL VALOR TOTAL. QUEDANDO ENTENDIDO QUE ES NULA CUALQUIER CLÁUSULA QUE CONTRAVENGA LO ANTERIOR. LA PRESENTE TENDRÁ CARÁCTER DE TÍTULO EJECUTIVO Y SU CUMPLIMIENTO SE EXIGIRÁ POR LA VÍA DE APREMIO. SOMETIÉNDOSE EXPRESAMENTE A LA JURISDICCIÓN Y COMPETENCIA DE LOS TRIBUNALES DEL DEPARTAMENTO DE FRANCISCO MORAZÁN."

Las garantías o fianzas emitidas a favor del BENEFICIARIO serán solidarias, incondicionales, irrevocables y de realización automática **y no deberán adicionarse cláusulas que anulen o limiten la cláusula obligatoria.**

Se entenderá por el incumplimiento si el Afianzado/Garantizado:

1. Retira su oferta durante el período de validez de la misma.
2. No acepta la corrección de los errores (si los hubiere) del Precio de la Oferta.
3. Si después de haber sido notificado de la aceptación de su Oferta por el Contratante durante el período de validez de la misma, no firma o rehúsa firmar el Contrato, o se rehúsa a presentar la Garantía de Cumplimiento.
4. Cualquier otra condición estipulada en el pliego de condiciones.

En fe de lo cual, se emite la presente Fianza/Garantía, en la ciudad de_____, Municipio de_____, a los _____ del mes de_____del año_____.

SELLO Y FIRMA AUTORIZADA

FORMATO *[GARANTIA/FIANZA]* DE CUMPLIMIENTO
[NOMBRE DE ASEGURADORA/BANCO]

[GARANTIA / FIANZA]
DE CUMPLIMIENTO Nº: _____

FECHA DE EMISION: _____

AFIANZADO/GARANTIZADO: _____

DIRECCION Y TELEFONO: _

[Garantía/Fianza] a favor de *[indicar el nombre de la institución a favor de la cual se extiende la garantía]*, para garantizar que el *[Afianzado/Garantizado]*, salvo fuerza mayor o caso fortuito debidamente comprobados, **CUMPLIRA** cada uno de los términos, cláusulas, responsabilidades y obligaciones estipuladas en el contrato firmado al efecto entre el *[Afianzado/Garantizado]* y el Beneficiario, para la Ejecución del Proyecto: "*[indicar el nombre de la licitación]*" ubicado en *[indicar la ubicación]*.

SUMA
AFIANZADA/ GARANTIZADA: _____

VIGENCIA **De:**_____ **Hasta:**_____

BENEFICIARIO: _____

Todas las garantías deberán incluir **textualmente** la siguiente cláusula obligatoria.

"LA PRESENTE GARANTÍA ES SOLIDARIA, INCONDICIONAL, IRREVOCABLE Y DE REALIZACIÓN AUTOMÁTICA, DEBIENDO SER EJECUTADA POR EL VALOR TOTAL DE LA MISMA, AL SIMPLE REQUERIMIENTO DEL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL (IHSS), ACOMPAÑADA DE LA RESOLUCIÓN ADMINISTRATIVA CORRESPONDIENTE, SIN NECESIDAD DE TRÁMITES PREVIOS AL MISMO. SIN PERJUICIO DE LOS AJUSTES QUE PUDIERAN HABER, SI FUERE EL CASO, QUE SE HARAN CON POSTERIORIDAD A LA ENTREGA DEL VALOR TOTAL. QUEDANDO ENTENDIDO QUE ES NULA CUALQUIER CLÁUSULA QUE CONTRAVENGA LO ANTERIOR. LA PRESENTE TENDRÁ CARÁCTER DE TÍTULO EJECUTIVO Y SU CUMPLIMIENTO SE EXIGIRÁ POR LA VÍA DE APREMIO. SOMETIÉNDOSE EXPRESAMENTE A LA JURISDICCIÓN Y COMPETENCIA DE LOS TRIBUNALES DEL DEPARTAMENTO DE FRANCISCO MORAZÁN."

Las garantías o fianzas emitidas a favor del BENEFICIARIO serán solidarias, incondicionales, irrevocables y de realización automática **y no deberán adicionarse cláusulas que anulen o limiten la cláusula obligatoria.**

Se entenderá por el incumplimiento si el Afianzado/Garantizado:

1. Retira su oferta durante el período de validez de la misma.
2. No acepta la corrección de los errores (si los hubiere) del Precio de la Oferta.
3. Si después de haber sido notificado de la aceptación de su Oferta por el Contratante durante el período de validez de la misma, no firma o rehúsa firmar el Contrato, o se rehúsa a presentar la Garantía de Cumplimiento.
4. Cualquier otra condición estipulada en el pliego de condiciones.

En fe de lo cual, se emite la presente Fianza/Garantía, en la ciudad de_____, Municipio de_____, a los_____del mes de_____del año_____.

SELLO Y FIRMA AUTORIZADA

Condiciones Generales del Contrato

Índice de Cláusulas

Condiciones Generales del Contrato

1. Definiciones

1.1. Las siguientes palabras y expresiones tendrán los significados que aquí se les asigna:

(a) "El Sitio del Proyecto", donde corresponde, significa el lugar citado en las **CEC**.

(b) "Contrato" significa el Contrato celebrado entre el Comprador y el Proveedor, junto con los documentos del Contrato allí referidos, incluyendo todos los anexos y apéndices, y todos los documentos incorporados allí por referencia.

(c) "Documentos del Contrato" significa los documentos enumerados en el Contrato, incluyendo cualquier enmienda.

(d) "Precio del Contrato" significa el precio pagadero al Proveedor según se especifica en el Contrato, sujeto a las condiciones y ajustes allí estipulados o deducciones propuestas, según corresponda en virtud del Contrato.

(e) "Día" significa día calendario.

(f) "Cumplimiento" significa que el Proveedor ha completado la prestación de los Servicios Conexos de acuerdo con los términos y condiciones establecidas en el Contrato.

(g) "CGC" significa las Condiciones Generales del Contrato.

(h) "Bienes" significa todos los productos, materia prima, maquinaria y equipo, y otros materiales que el Proveedor deba proporcionar al Comprador en virtud del Contrato.

(j) "Comprador" significa la entidad que compra los Bienes y Servicios Conexos, según se indica en las **CEC**.

(k) "Servicios Conexos" significan los servicios incidentales relativos a la provisión de los bienes, tales como transporte, seguro, instalación, puesta en

servicio, capacitación y mantenimiento inicial y otras obligaciones similares del Proveedor en virtud del Contrato.

(l) "CEC" significa las Condiciones Especiales del Contrato.

(m) "Subcontratista" significa cualquier persona natural, entidad privada con quienes el Proveedor ha subcontratado el suministro de cualquier porción de los Bienes o la ejecución de cualquier parte de los Servicios.

(n) "Proveedor" significa la persona natural, jurídica cuya oferta para ejecutar el contrato ha sido aceptada por el Comprador y es denominada como tal en el Contrato.

2. Documentos del Contrato

2.1 Sujetos al orden de precedencia establecido en el Contrato, se entiende que todos los documentos que forman parte integral del Contrato (y todos sus componentes allí incluidos) son correlativos, complementarios y recíprocamente aclaratorios. El Contrato deberá leerse de manera integral.

3. Fraude y Corrupción

3.1 El Estado Hondureño exige a todos los organismos ejecutores y organismos contratantes, al igual que a todas las firmas, entidades o personas oferentes por participar o participando en procedimientos de contratación, incluyendo, entre otros, solicitantes, oferentes, contratistas, consultores y concesionarios (incluyendo sus respectivos funcionarios, empleados y representantes), observar los más altos niveles éticos durante el proceso de selección y las negociaciones o la ejecución de un contrato. Los actos de fraude y corrupción están prohibidos.

3.2 El Comprador, así como cualquier instancia de control del Estado Hondureño tendrán el derecho revisar a los Oferentes, proveedores, contratistas, subcontratistas, consultores y concesionarios sus cuentas y registros y cualesquiera otros documentos relacionados con la presentación de propuestas y con el cumplimiento del contrato y someterlos a una auditoría por auditores designados por el Comprador, o la respectiva instancia de control del Estado Hondureño. Para estos efectos, el Proveedor y sus subcontratistas deberán: (i) conserven todos los documentos y registros relacionados con este Contrato por un período de tres (5) años luego de terminado el trabajo contemplado en el Contrato; y (ii) entreguen todo

documento necesario para la investigación de denuncias de fraude o corrupción, y pongan a la disposición del Comprador o la respectiva instancia de control del Estado Hondureño, los empleados o agentes del Proveedor y sus subcontratistas que tengan conocimiento del Contrato para responder las consultas provenientes de personal del Comprador o la respectiva instancia de control del Estado Hondureño o de cualquier investigador, agente, auditor o consultor apropiadamente designado para la revisión o auditoría de los documentos. Si el Proveedor o cualquiera de sus subcontratistas incumple el requerimiento del Comprador o la respectiva instancia de control del Estado Hondureño, o de cualquier otra forma obstaculiza la revisión del asunto por éstos, el Comprador o la respectiva instancia de control del Estado Hondureño bajo su sola discreción, podrá tomar medidas apropiadas contra el Proveedor o subcontratista para asegurar el cumplimiento de esta obligación.

3.3 Los actos de fraude y corrupción son sancionados por la Ley de Contratación del Estado, sin perjuicio de la responsabilidad en que se pudiera incurrir conforme al Código Penal.

4. Interpretación

4.1 Si el contexto así lo requiere, el singular significa el plural, y viceversa.

4.2 Incoterms

(a) 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.

(b) El término DDP, DPA y otros similares, cuando se utilicen, se regirán por lo establecido en la edición vigente de los Incoterms especificada en la CEC, y publicada por la Cámara de Comercio Internacional en París, Francia.

4.3 Totalidad del Contrato

El Contrato constituye la totalidad de lo acordado entre el Comprador y el Proveedor y substituye todas las comunicaciones, negociaciones y acuerdos (ya sea escritos o verbales) realizados entre las partes con anterioridad a la fecha de la celebración del Contrato.

4.4 Enmienda

Ninguna enmienda u otra variación al Contrato será válida a

menos que esté por escrito, fechada y se refiera expresamente al Contrato, y esté firmada por un representante de cada una de las partes debidamente autorizado.

4.5 Limitación de Dispensas

(a) Sujeto a lo indicado en la Sub cláusula 4.5(b) siguiente de estas CGC, ninguna dilación, tolerancia, 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 dispensa concedida por cualquiera de las partes por un incumplimiento del Contrato, servirá de dispensa para incumplimientos posteriores o continuos del Contrato.

(b) Toda dispensa a los derechos, poderes o remedios de una de las partes en virtud del Contrato, deberá ser por escrito, llevar la fecha y estar firmada por un representante autorizado de la parte otorgando dicha dispensa y deberá especificar la obligación que está dispensando y el alcance de la dispensa.

4.6 Divisibilidad

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.

5. Idioma

5.1 El Contrato, así como toda la correspondencia y documentos relativos al Contrato intercambiados entre el Proveedor y el Comprador, deberán ser escritos en español. Los documentos de sustento y material impreso que formen parte del Contrato, pueden estar en otro idioma siempre que los mismos estén acompañados de una traducción fidedigna de los apartes pertinentes al español y, en tal caso, dicha traducción prevalecerá para efectos de interpretación del Contrato.

5.2 El Proveedor será responsable de todos los costos de la traducción al idioma que rige, así como de todos los riesgos derivados de la exactitud de dicha traducción de los

documentos proporcionados por el Proveedor.

6. Consorcio

6.1 Si el Proveedor es un Consorcio, todas las partes que lo conforman deberán ser mancomunada y solidariamente responsables frente al Comprador por el cumplimiento de las disposiciones del Contrato y deberán designar a una de ellas para que actúe como representante con autoridad para comprometer al Consorcio. La composición o constitución del Consorcio no podrá ser alterada sin el previo consentimiento del Comprador.

7. Elegibilidad

7.1 El Proveedor y sus Subcontratistas deberán tener plena capacidad de ejercicio, y no hallarse comprendidos en alguna de las circunstancias siguientes:

(a) Haber sido condenados mediante sentencia firme por delitos contra la propiedad, delitos contra la fe pública, cohecho, enriquecimiento ilícito, negociaciones incompatibles con el ejercicio de funciones públicas, malversación de caudales públicos o contrabando y defraudación fiscal, mientras subsista la condena. Esta prohibición también es aplicable a las sociedades mercantiles u otras personas jurídicas cuyos administradores o representantes se encuentran en situaciones similares por actuaciones a nombre o en beneficio de las mismas;

(b) Haber sido declarado en quiebra o en concurso de acreedores, mientras no fueren rehabilitados;

(c) Ser funcionarios o empleados, con o sin remuneración, al servicio de los Poderes del Estado o de cualquier institución descentralizada, municipalidad u organismo que se financie con fondos públicos, sin perjuicio de lo previsto en el Artículo 258 de la Constitución de la República;

(d) Haber dado lugar, por causa de la que hubiere sido declarado culpable, a la resolución firme de cualquier contrato celebrado con la Administración o a la suspensión temporal en el Registro de Proveedores y Contratistas en tanto dure la sanción. En el primer caso, la prohibición de contratar tendrá una duración de dos (2) años, excepto en aquellos casos en que haya sido objeto de resolución en sus contratos en dos ocasiones, en cuyo caso la prohibición de contratar será definitiva;

(e) Ser cónyuge, persona vinculada por unión de hecho o parientes dentro del cuarto grado de consanguinidad o

segundo de afinidad de cualquiera de los funcionarios o empleados bajo cuya responsabilidad esté la precalificación de las empresas, la evaluación de las propuestas, la adjudicación o la firma del contrato;

(f) Tratarse de sociedades mercantiles en cuyo capital social participen funcionarios o empleados públicos que tuvieren influencia por razón de sus cargos o participaren directa o indirectamente en cualquier etapa de los procedimientos de selección de contratistas. Esta prohibición se aplica también a las compañías que cuenten con socios que sean cónyuges, personas vinculadas por unión de hecho o parientes dentro del cuarto grado de consanguinidad o segundo de afinidad de los funcionarios o empleados a que se refiere el numeral anterior, o aquellas en las que desempeñen, puestos de dirección o de representación personas con esos mismos grados de relación o de parentesco;

(g) Haber intervenido directamente o como asesores en cualquier etapa de los procedimientos de contratación o haber participado en la preparación de las especificaciones, planos, diseños o términos de referencia, excepto en actividades de supervisión de construcción; e,

(h) Estar suspendido del Registro de Proveedores y Contratistas o tener vigente sanción de suspensión para participar en procedimientos de contratación administrativa.

8. Notificaciones

8.1 Todas las notificaciones entre las partes en virtud de este Contrato deberán ser por escrito y dirigidas a la dirección indicada en las **CEC**. El término "por escrito" significa comunicación en forma escrita con prueba de recibo.

8.2 Una notificación será efectiva en la fecha más tardía entre la fecha de entrega y la fecha de la notificación.

9. Ley aplicable

9.1 El Contrato se regirá y se interpretará según las leyes Hondureñas.

10. Solución de controversias

10.1 El Comprador y el Proveedor harán todo lo posible para resolver amigablemente mediante negociaciones directas informales, cualquier desacuerdo o controversia que se haya suscitado entre ellos en virtud o en referencia al Contrato.

10.2 Cualquier divergencia que se presente sobre un asunto que no se resuelva mediante un arreglo entre el Proveedor y el Comprador, deberá ser resuelto por éste, quien previo

estudio del caso dictará su resolución y la comunicará al reclamante.

10.3 Contra la resolución del Comprador quedará expedita la vía judicial ante los tribunales de lo Contencioso Administrativo, salvo que las **CEC** establezcan la posibilidad de acudir al Arbitraje.

11. Alcance de los suministros

11.1 Los Bienes y Servicios Conexos serán suministrados según lo estipulado en la Lista de Requisitos.

12. Entrega y documentos

12.1 Sujeto a lo dispuesto en la Sub cláusula 32.1 de las CGC, la Entrega de los Bienes y Cumplimiento de los Servicios Conexos se realizará de acuerdo con el Plan de Entrega y Cronograma de Cumplimiento indicado en la Lista de Requisitos. Los detalles de los documentos que deberá suministrar el Proveedor se especifican en las **CEC**.

13. Responsabilidades del Proveedor

13.1 El Proveedor deberá proporcionar todos los bienes y Servicios Conexos incluidos en el Alcance de Suministros de conformidad con la Cláusula 11 de las CGC y el Plan de Entrega y Cronograma de Cumplimiento, de conformidad con la Cláusula 12 de las CGC.

14. Precio del Contrato

14.1 Los precios que cobre el Proveedor por los Bienes proporcionados y los Servicios Conexos prestados en virtud del contrato no podrán ser diferentes de los cotizados por el Proveedor en su oferta, excepto por cualquier ajuste de precios autorizado en las **CEC**.

15. Condiciones de Pago

15.1 El precio del Contrato se pagará según se establece en las **CEC**.

15.2 La solicitud de pago del Proveedor al Comprador deberá ser por escrito, acompañada de documentación de soporte que describan, según corresponda, los Bienes entregados y los Servicios Conexos cumplidos, y de los documentos presentados de conformidad con las Cláusulas 7.4 y 12 de las CGC y en cumplimiento de las obligaciones estipuladas en el Contrato.

15.3 El Comprador efectuará los pagos prontamente, pero de ninguna manera podrá exceder sesenta (60) días después de la presentación de una factura o solicitud de pago por el Proveedor, y después de que el Comprador la haya

aceptado.

15.4 Las monedas en que se le pagará al Proveedor en virtud de este Contrato serán aquellas que el Proveedor hubiese especificado en su oferta.

15.5 Si el Comprador no efectuara cualquiera de los pagos al Proveedor en las fechas de vencimiento correspondiente o dentro del plazo establecido en las **CEC**, el Comprador pagará al Proveedor interés sobre los montos de los pagos morosos a la tasa de interés establecida en las **CEC**, por el período de la demora hasta que haya efectuado el pago completo, ya sea antes o después de cualquier juicio o fallo de arbitraje.

16. Impuestos y derechos

16.1 El Proveedor será totalmente responsable por todos los impuestos, gravámenes, timbres, comisiones por licencias, y otros cargos similares incurridos hasta la entrega de los Bienes contratados con el Comprador.

16.2 El Comprador interpondrá sus mejores oficios para que el Proveedor se beneficie con el mayor alcance posible de cualquier exención impositiva, concesiones, o privilegios legales que pudiesen aplicar al Proveedor en Honduras.

17. Garantía Cumplimiento

17.1 El Proveedor, dentro de los siguientes treinta (30) días de la notificación de la adjudicación del Contrato, deberá suministrar la Garantía de Cumplimiento del Contrato por el monto equivalente al quince por ciento (15%) del valor del contrato.

17.2 Los recursos de la Garantía de Cumplimiento serán pagaderos al Comprador como indemnización por cualquier pérdida que le pudiera ocasionar el incumplimiento de las obligaciones del Proveedor en virtud del Contrato.

17.3 Como se establece en las **CEC**, la Garantía de Cumplimiento, si es requerida, deberá estar denominada en la(s) misma(s) moneda(s) del Contrato, o en una moneda de libre convertibilidad aceptable al Comprador, y presentada en una de los formatos estipuladas por el Comprador en las **CEC**, u en otro formato aceptable al Comprador.

17.4 La validez de la Garantía de Cumplimiento excederá en tres (3) meses la fecha prevista de culminación de la entrega de los bienes.

17.5 Efectuada que fuere la entrega de los bienes y realizada la liquidación del contrato, cuando se establezca en las **CEC**, el Proveedor sustituirá la garantía de cumplimiento del contrato por una garantía de calidad de los bienes suministrados, con vigencia por el tiempo previsto en las **CEC** y cuyo monto será equivalente al cinco por ciento (5%) del valor del Contrato.

18. Derechos de Autor

18.1 Los derechos de autor de todos los planos, documentos y otros materiales conteniendo datos e información proporcionada al Comprador por el Proveedor, seguirán siendo de propiedad del Proveedor. Si esta información fue suministrada al Comprador directamente o a través del Proveedor por terceros, incluyendo proveedores de materiales, el derecho de autor de dichos materiales seguirá siendo de propiedad de dichos terceros.

19. Confidencialidad de la Información

19.1 El Comprador y el Proveedor deberán mantener confidencialidad y en ningún momento divulgarán a terceros, sin el consentimiento por escrito 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, lo anterior, el Proveedor podrá proporcionar a sus Subcontratistas los documentos, datos e información recibidos del Comprador 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 del Proveedor bajo la Cláusula 19 de las CGC.

19.2 El Comprador no utilizará dichos documentos, datos u otra información recibida del Proveedor para ningún uso que no esté relacionado con el Contrato. Asimismo, el Proveedor no utilizará los documentos, datos u otra información recibida del Comprador para ningún otro propósito que el de la ejecución del Contrato.

19.3 La obligación de las partes de conformidad con las Sub cláusulas19.1 y 19.2 de las CGC arriba mencionadas, no aplicará a información que:

(a) el Comprador o el Proveedor requieran compartir con el Banco u 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 obtenida previamente directa o indirectamente de la otra parte; o

(d) que de otra manera fue legalmente puesta a la disponibilidad de esa parte por una tercera parte que no tenía obligación de confidencialidad.

19.4 Las disposiciones precedentes de esta cláusula 19 de las CGC 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.

19.5 Las disposiciones de la Cláusula 19 de las CGC permanecerán válidas después del cumplimiento o terminación del contrato por cualquier razón.

20. subcontratación

20.1 El Proveedor informará al Comprador por escrito de todos los subcontratos que adjudique en virtud del Contrato si no los hubiera especificado en su oferta. Dichas notificaciones, en la oferta original o posterior, no eximirán al Proveedor de sus obligaciones, deberes y compromisos o responsabilidades contraídas en virtud del Contrato.

20.2 Todos los subcontratos deberán cumplir con las disposiciones de las Cláusulas 3 y 7 de las CGC.

21. Especificaciones y Normas

21.1 Especificaciones Técnicas y Planos

(a) Los Bienes y Servicios Conexos proporcionados bajo este contrato deberán ajustarse a las especificaciones técnicas y a las normas estipuladas en la Sección VI, Lista de Requisitos y, cuando no se hace referencia a una norma aplicable, la norma será equivalente o superior a las normas oficiales cuya aplicación sea apropiada en el país de origen de los Bienes.

(b) 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 del Comprador, mediante notificación al Comprador de dicho rechazo.

(c) Cuando en el Contrato se hagan referencias a códigos y normas conforme a las cuales éste debe ejecutarse, la edición o versión revisada de dichos códigos y normas será la especificada en la Lista de Requisitos. Cualquier cambio de dichos códigos o normas durante la ejecución del Contrato se aplicará solamente con la aprobación previa del Comprador y dicho cambio se regirá de conformidad con la Cláusula 32 de las CGC.

22. Embalaje y Documentos

22.1 El Proveedor embalará los bienes en la forma necesaria para impedir que se dañen o deterioren durante el transporte al lugar de destino final indicado en el Contrato. El embalaje deberá ser adecuado para resistir, sin limitaciones, su manipulación brusca y descuidada, su exposición a temperaturas extremas, la sal y las precipitaciones, y su almacenamiento en espacios abiertos. En el tamaño y peso de los embalajes se tendrá en cuenta, cuando corresponda, la lejanía del lugar de destino final de los bienes y la carencia de equipo pesado de carga y descarga en todos los puntos en que los bienes deban transbordarse.

22.2 El embalaje, las identificaciones y los documentos que se coloquen dentro y fuera de los bultos deberán cumplir estrictamente con los requisitos especiales que se hayan estipulado expresamente en el Contrato, y cualquier otro requisito, si los hubiere, especificado en las **CEC** y en cualquiera otra instrucción dispuesta por el Comprador.

23. Seguros

23.1 A menos que se disponga otra cosa en las **CEC**, los Bienes suministrados bajo el Contrato deberán estar completamente asegurados, en una moneda de libre convertibilidad de un país elegible, contra riesgo de extravío o daños incidentales ocurridos durante fabricación, adquisición, transporte, almacenamiento y entrega, de conformidad con los *Incoterms* aplicables **o según se disponga en las CEC**.

24. Transporte

24.1 A menos que se disponga otra cosa en las **CEC**, la responsabilidad por los arreglos de transporte de los Bienes se regirá por los *Incoterms* indicados.

25. Inspecciones y Pruebas

25.1 El Proveedor realizará todas las pruebas y/o inspecciones de los Bienes y Servicios Conexos según se dispone en las **CEC**, por su cuenta y sin costo alguno para el Comprador.

25.2 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 los

Bienes o en otro lugar en Honduras. De conformidad con la Sub cláusula 25.3 de las CGC, cuando dichas inspecciones o pruebas sean realizadas en recintos del Proveedor o de sus subcontratistas se les proporcionarán a los inspectores todas las facilidades y asistencia razonables, incluso el acceso a los planos y datos sobre producción, sin cargo alguno para el Comprador.

25.3 El Comprador o su representante designado tendrá derecho a presenciar las pruebas y/o inspecciones mencionadas en la Sub cláusula 25.2 de las CGC, siempre y cuando éste asuma todos los costos y gastos que ocasione su participación, incluyendo gastos de viaje, alojamiento y alimentación.

25.4 Cuando el Proveedor esté listo para realizar dichas pruebas e inspecciones, notificará oportunamente al Comprador 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 Comprador o a su representante designado presenciar las pruebas o inspecciones, cuando el proveedor esté dispuesto.

25.5 El Comprador 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. 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.

25.6 El Proveedor presentará al Comprador un informe de los resultados de dichas pruebas y/o inspecciones.

25.7 El Comprador 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 el Comprador. Asimismo, tendrá que repetir las

pruebas o inspecciones, sin ningún costo para el Comprador, una vez que notifique al Comprador de conformidad con la Sub cláusula 25.4 de las CGC.

25.8 El Proveedor acepta que ni la realización de pruebas o inspecciones de los Bienes o de parte de ellos, ni la presencia del Comprador o de su representante, ni la emisión de informes, de conformidad con la Sub cláusula 25.6 de las CGC, lo eximirán de las garantías u otras obligaciones en virtud del Contrato.

26. Liquidación por Daños y Perjuicios

26.1 Con excepción de lo que se establece en la Cláusula 31 de las CGC, si el Proveedor no cumple con la entrega de la totalidad o parte de los Bienes en la(s) fecha(s) establecida(s) o con la prestación de los Servicios Conexos dentro del período especificado en el Contrato, sin perjuicio de los demás recursos que el Comprador tenga en virtud del Contrato, éste podrá deducir del Precio del Contrato por concepto de liquidación de daños y perjuicios, una suma equivalente al porcentaje del precio de entrega de los bienes atrasados o de los servicios no prestados establecido en las **CEC** por cada día de retraso hasta alcanzar el máximo del porcentaje especificado en esas **CEC**. Al alcanzar el máximo establecido, el Comprador podrá dar por terminado el contrato de conformidad con la Cláusula 34 de las CGC.

27. Garantía de los Bienes

27.1 El Proveedor garantiza que todos los bienes suministrados en virtud del Contrato son nuevos, sin uso, del modelo más reciente o actual e incorporan todas las mejoras recientes en cuanto a diseño y materiales, a menos que el Contrato disponga otra cosa.

27.2 De conformidad con la Sub cláusula 21.1(b) de las CGC, el Proveedor garantiza que todos los bienes suministrados estarán libres de defectos derivados de actos y omisiones que éste hubiese incurrido, o derivados del diseño, materiales o manufactura, durante el uso normal de los bienes en las condiciones que imperen en el país de destino final.

27.3 Salvo que se indique otra cosa en las **CEC,** la garantía permanecerá vigente durante el período cuya fecha de terminación sea la más temprana entre los períodos siguientes: doce (12) meses a partir de la fecha en que los bienes, o cualquier parte de ellos según el caso, hayan sido entregados y aceptados en el punto final de destino indicado en el Contrato, o dieciocho (18) meses a partir de la fecha de

embarque en el puerto o lugar de flete en el país de origen.

27.4 El Comprador comunicará al Proveedor la naturaleza de los defectos y proporcionará toda la evidencia disponible, inmediatamente después de haberlos descubierto. El Comprador otorgará al Proveedor facilidades razonables para inspeccionar tales defectos.

27.5 Tan pronto reciba el Proveedor dicha comunicación, y dentro del plazo establecido en las **CEC**, deberá reparar o reemplazar de forma expedita los Bienes defectuosos, o sus partes sin ningún costo para el Comprador.

27.6 Si el Proveedor después de haber sido notificado, no cumple con corregir los defectos dentro del plazo establecido, el Comprador, dentro de un tiempo razonable, podrá proceder a tomar las medidas necesarias para remediar la situación, por cuenta y riesgo del Proveedor y sin perjuicio de otros derechos que el Comprador pueda ejercer contra el Proveedor en virtud del Contrato.

28. Indemnización por Derechos de Patente

28.1 El Proveedor indemnizará y librará de toda responsabilidad al Comprador y 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 el Comprador tenga que incurrir como resultado de transgresión o supuesta transgresión de derechos de patente, uso de modelo, diseño registrado, marca registrada, derecho 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 el País donde está el lugar del proyecto; 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 resulte 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.

28.2 Si se entablara un proceso legal o una demanda contra el Comprador como resultado de alguna de las situaciones indicadas en la Sub cláusula 28.1 de las CGC, el Comprador notificará prontamente al Proveedor y éste por su propia cuenta y en nombre del Comprador responderá a dicho proceso o demanda, y realizará las negociaciones necesarias para llegar a un acuerdo de dicho proceso o demanda.

28.3 Si el Proveedor no notifica al Comprador dentro de veintiocho (28) días a partir del recibo de dicha comunicación de su intención de proceder con tales procesos o reclamos, el Comprador tendrá derecho a emprender dichas acciones en su propio nombre. El Comprador será reembolsado por el Proveedor por las costas procesales en que hubiera incurrido.

28.4 El Comprador se compromete, a solicitud del Proveedor, a prestarle toda la asistencia posible para que el Proveedor pueda contestar las citadas acciones legales o reclamaciones. El Comprador será reembolsado por el Proveedor por todos los gastos razonables en que hubiera incurrido.

28.5 El Comprador 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 el Comprador o a nombre suyo.

29. Limitación de Responsabilidad

29.1 Excepto en casos de negligencia grave o actuación de mala fe,

(a) el Proveedor no tendrá ninguna responsabilidad contractual, de agravio o de otra índole frente al

Comprador 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 al Comprador los daños y perjuicios previstos en el Contrato, y

(b) la responsabilidad total del Proveedor frente al Comprador, ya sea contractual, de agravio o de otra índole, no podrá exceder el Precio del Contrato, entendiéndose que tal limitación de responsabilidad no se aplicará a los costos provenientes de la reparación o reemplazo de equipo defectuoso, ni afecta la obligación del Proveedor de indemnizar al Comprador por las transgresiones de patente.

30. Cambio en las Leyes y Regulaciones

30.1 A menos que se indique otra cosa en el Contrato, si después de la fecha de 28 días antes de la presentación de Ofertas, cualquier ley, reglamento, decreto, ordenanza o estatuto con carácter de ley entrase en vigencia, se promulgase, abrogase o se modificase en el lugar de Honduras donde está ubicado el Proyecto (incluyendo cualquier cambio en interpretación o aplicación por las autoridades competentes) y que afecte posteriormente la fecha de Entrega y/o el Precio del Contrato, dicha Fecha de Entrega y/o Precio del Contrato serán incrementados o reducidos según corresponda, en la medida en que el Proveedor haya sido afectado por estos cambios en el desempeño de sus obligaciones en virtud del Contrato. No obstante, lo anterior, dicho incremento o disminución del costo no se pagará separadamente ni será acreditado si el mismo ya ha sido tenido en cuenta en las provisiones de ajuste de precio, si corresponde y de conformidad con la Cláusula 14 de las CGC.

31. Fuerza Mayor

31.1 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.

31.2 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 Proveedor. Tales eventos pueden incluir sin que éstos sean los únicos, actos del Comprador en su

capacidad soberana, guerras o revoluciones, incendios, inundaciones, epidemias, restricciones de cuarentena, y embargos de cargamentos.

31.3 Si se presentara un evento de Fuerza Mayor, el Proveedor notificará por escrito al Comprador a la máxima brevedad posible sobre dicha condición y causa. A menos que el Comprador 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.

32. Órdenes de Cambio y Enmiendas al Contrato

32.1 El Comprador podrá, en cualquier momento, efectuar cambios dentro del marco general del Contrato, mediante orden escrita al Proveedor de acuerdo con la Cláusula 8 de las CGC, en uno o más de los siguientes aspectos:

(a) planos, diseños o especificaciones, cuando los Bienes que deban suministrarse en virtud al Contrato deban ser fabricados específicamente para el Comprador;

(b) la forma de embarque o de embalaje;

(c) el lugar de entrega, y/o

(d) los Servicios Conexos que deba suministrar el Proveedor.

32.2 Si cualquiera de estos cambios causara un aumento o disminución en el costo o en el tiempo necesario para que el Proveedor cumpla cualquiera de las obligaciones en virtud del Contrato, se efectuará un ajuste equitativo al Precio del Contrato o al Plan de Entregas/de Cumplimiento, o a ambas cosas, y el Contrato se enmendará según corresponda. El Proveedor deberá presentar la solicitud de ajuste de conformidad con esta Cláusula, dentro de los veintiocho (28) días contados a partir de la fecha en que éste reciba la solicitud de la orden de cambio del Comprador.

32.3 Los precios que cobrará el Proveedor por Servicios Conexos que pudieran ser necesarios pero que no fueron incluidos en el Contrato, deberán convenirse previamente entre las partes, y no excederán los precios que el Proveedor cobra actualmente a terceros por servicios similares.

32.4 Sujeto a lo anterior, no se introducirá ningún cambio o

modificación al Contrato excepto mediante una enmienda por escrito ejecutada por ambas partes.

33. Prórroga de los Plazos

33.1 Si en cualquier momento durante la ejecución del Contrato, el Proveedor o sus Subcontratistas encontrasen condiciones que impidiesen la entrega oportuna de los Bienes o el cumplimiento de los Servicios Conexos de conformidad con la Cláusula 12 de las CGC, el Proveedor informará prontamente y por escrito al Comprador sobre la demora, posible duración y causa. Tan pronto como sea posible después de recibir la comunicación del Proveedor, el Comprador evaluará la situación y a su discreción podrá prorrogar el plazo de cumplimiento del Proveedor. En dicha circunstancia, ambas partes ratificarán la prórroga mediante una enmienda al Contrato.

33.2 Excepto en el caso de Fuerza Mayor, como se indicó en la Cláusula 31 de las CGC, cualquier retraso en el desempeño de sus obligaciones de Entrega y Cumplimiento expondrá al Proveedor a la imposición de liquidación por daños y perjuicios de conformidad con la Cláusula 26 de las CGC, a menos que se acuerde una prórroga en virtud de la Sub cláusula 33.1 de las CGC.

34. Terminación

34.1 Terminación por Incumplimiento

(a) El Comprador, sin perjuicio de otros recursos a su haber en caso de incumplimiento del Contrato, podrá terminar el Contrato en su totalidad o en parte mediante una comunicación de incumplimiento por escrito al Proveedor 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 el Comprador de conformidad con la Cláusula 33 de las CGC; o

(ii) Si el Proveedor no cumple con cualquier otra obligación en virtud del Contrato; o

(iii) Si el Proveedor, a juicio del Comprador, durante el proceso de licitación o de ejecución del Contrato, ha participado en actos de fraude y corrupción, según se define en la Cláusula 3 de las CGC; o

(iv) La disolución de la sociedad mercantil

Proveedora, salvo en los casos de fusión de sociedades y siempre que solicite de manera expresa al Comprador su autorización para la continuación de la ejecución del contrato, dentro de los diez días hábiles siguientes a la fecha en que tal fusión ocurra. El Comprador podrá aceptar o denegar dicha solicitud, sin que, en este último caso, haya derecho a indemnización alguna; o

(v) La falta de constitución de la garantía de cumplimiento del contrato o de las demás garantías a cargo del Proveedor dentro de los plazos correspondientes;

(b) En caso de que el Comprador termine el Contrato en su totalidad o en parte, de conformidad con la Cláusula 34.1(a) de las CGC, éste podrá adquirir, bajo términos y condiciones que considere apropiadas, Bienes o Servicios Conexos similares a los no suministrados o prestados. En estos casos, el Proveedor deberá pagar al Comprador los costos adicionales resultantes de dicha adquisición. Sin embargo, el Proveedor seguirá estando obligado a completar la ejecución de aquellas obligaciones en la medida que hubiesen quedado sin concluir.

34.2 Terminación por Insolvencia

(a) El Comprador podrá rescindir el Contrato en cualquier momento mediante comunicación por escrito al Proveedor en caso de la declaración de quiebra, disminución en los ingresos percibidos o su comprobada incapacidad financiera. Igual sucederá en caso de recorte presupuestarios de fondos nacionales que se efectúe por razón de la situación económica y financiera del país, la estimación de la percepción de ingresos menores a los gastos proyectados y en caso de necesidades imprevistas o de emergencia, lo anterior en cumplimiento del Artículo 69 del Decreto N°141-2017 que contiene el Presupuesto de Ingresos de La Administración Pública para el año 2018 publicado el 19 de enero de 2018, en la Gaceta Diario Oficial de la República.

34.3 Terminación por Conveniencia.

(a) El Comprador, mediante comunicación enviada al Proveedor, podrá terminar el Contrato total o parcialmente, en cualquier momento por razones de conveniencia. La comunicación de terminación deberá indicar que la terminación es por conveniencia del Comprador, el alcance de la terminación de las responsabilidades del Proveedor en virtud del Contrato y la fecha de efectividad de dicha terminación.

(b) Los bienes que ya estén fabricados y listos para embarcar dentro de los veintiocho (28) días siguientes a al recibo por el Proveedor de la notificación de terminación del Comprador deberán ser aceptados por el Comprador de acuerdo con los términos y precios establecidos en el Contrato. En cuanto al resto de los Bienes el Comprador 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 el balance restante y se pague al Proveedor una suma convenida por aquellos Bienes o Servicios Conexos que hubiesen sido parcialmente completados y por los materiales y repuestos adquiridos previamente por el Proveedor.

34.4 El Comprador podrá terminar el Contrato también en caso de muerte del Proveedor individual, salvo que los herederos ofrezcan concluir con el mismo con sujeción a todas sus estipulaciones; la aceptación de esta circunstancia será potestativa del Comprador sin que los herederos tengan derecho a indemnización alguna en caso contrario.

34.5 El contrato también podrá ser terminado por el mutuo acuerdo de las partes.

35. Cesión

35.1 Ni el Comprador ni el Proveedor podrán ceder total o parcialmente las obligaciones que hubiesen contraído en virtud del Contrato, excepto con el previo consentimiento por escrito de la otra parte.

Condiciones Especiales del Contrato

Las siguientes Condiciones Especiales del Contrato (CEC) complementarán y/o enmendarán las Condiciones Generales del Contrato (CGC). En caso de haber conflicto, las provisiones aquí dispuestas prevalecerán sobre las de las CGC.

[El Comprador seleccionará la redacción que corresponda utilizando los ejemplos indicados a continuación u otra redacción aceptable y suprimirá el texto en letra cursiva]

CGC 1.1(i)	El comprador es: El Instituto Hondureño de Seguridad Social (IHSS), y esta licitación se financiara con fondos del IHSS.
CGC 1.1(a)	*La entrega del equipo y componentes de los lotes 1, 2, 3, 4, y 5; para la* "Adquisición de Solución de Comunicación Core Firewall Interno, Switches de Acceso, Certificación y Reparación de Fibra Óptica, Solución de Seguridad Perimetral de Próxima Generación, Solución de Comunicación de Telefonía IP para el IHSS". Será en la*:* **Gerencia de Tecnología de Información y Comunicaciones, 8 Piso, Edificio Administrativo, IHSS, Barrio Abajo, Tegucigalpa. M.D.C.; con un representante del Almacen Central del IHSS.**
CGC 4.2 (b)	La versión de la edición de los Incoterms será*:* ***No aplica***
CGC 8.1	Para **notificaciones,** la dirección del Comprador será: Atención: **Dr. Richard Zablah** Director Ejecutivo Interino del IHSS Bo. Abajo, Edificio Administrativo del IHSS, 10 piso, Tegucigalpa, M.D.C., Honduras, C.A. Teléfono: 2222-8412
CGC 10.3	Agotada la vía administrativa, las controversias que generen los actos administrativos de esto contrato, se presentarán ante los Tribunales de Justicia de Francisco Morazán, para lo cual se requerirá resolución de autorización por parte de la Comisión Interventora del IHSS.
CGC 12.1	Detalle de los documentos que deben ser proporcionados por el Proveedor son: Factura o Recibo original del Proveedor a nombre del Instituto Hondureño de Seguridad Social, en que se indiquen la descripción del servicio. (i) Factura por equipos a nombre del Instituto Hondureño de Seguridad Social; recibo por servicios de instalación y capacitación. (ii) Informe de contratista indicando que en la Gerencia de Tecnología

	de Información y Comunicación, el servicio se ha prestado al IHSS, de acuerdo a lo establecido en el contrato, con el visto bueno de la supervisión designada para el contrato. (iii) Copia del contrato. (iv) Primer pago copia de garantía de cumplimiento y calidad.
CGC 15.1	**Modelo de disposición:** El pago del servicio se hará después de haber prestado el servicio así: Lote 1, 2, 3, 4 y 5 pago único conforme a entrega, será pagada por el INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL y sin recargo alguno, dicho pago y se efectuará en moneda de curso legal en Honduras (Lempira). El Instituto Hondureño de Seguridad Social**,** a través de la Gerencia Administrativa y Financiera, efectuará los trámites de pago conforme a los procedimientos establecidos por el INSTITUTO.
CGC 15.5	El plazo de pago después del cual el Comprador deberá pagar interés al Proveedor: **No aplica.**
CGC 17.3	Se requerirá" una Garantía de Cumplimiento Si se requiere una Garantía de Cumplimiento, del 15% del monto total del contrato; ésta deberá presentarse en la forma de: *fianza o garantía bancarias emitidas por una institución debidamente autorizada por la Comisión Nacional,* Vigente hasta tres (3) meses después del plazo previsto de prestación de servicios para el primer año. Si se requiere una Garantía de Cumplimiento, ésta deberá estar denominada en lempiras
CGC 17.5	*Se requerirá" la presentación de* una Garantía de Calidad, del 5% del monto total de los equipos contemplados en el contrato, vigente por un año a partir de la fecha del acta de recepción provisional final.
CGC 25.1	No Aplica
CGC 25.2	El personal de la Gerencia de Tecnología de Información y Comunicación, verificará el cumplimiento de todas las condiciones del contrato
CGC 26.1	El valor de la liquidación por daños y perjuicios será en concepto de multa el 0.36%; por cada día de atraso en entrega de equipos y/o servicios de soporte solicitados. Si la demora no justificada diera lugar a que el total cobrado por la multa aquí establecida ascendiera al diez por ciento (10%) del valor parcial de este contrato "EL INSTITUTO", podrá considerar la resolución total del contrato y hacer efectiva la garantía de cumplimiento, sin incurrir por esto en ninguna responsabilidad de su parte.

1. Contrato

"Contrato de Solución de Comunicación Core Firewall Interno, Switches de Acceso, Certificación y Reparación de Fibra Óptica, Solución de Seguridad Perimetral de Próxima Generación, Solución de Comunicación de Telefonía IP y Sistemas de Cámara de Video Vigilancia para el IHSS". , Celebrado entre el IHSS y La Empresa XXXX"

Nosotros **RICHARD ZABLAH ASFURA,** mayor de edad, casado, Doctor en Química y Farmacia, hondureño con Tarjeta de Identidad Nº0801-1944-02465 y de este domicilio, actuando en mi condición de Director Ejecutivo Interino del Instituto Hondureño de Seguridad Social (IHSS), entidad con Personería Jurídica creada mediante Decreto Legislativo Nº140 de fecha 19 de mayo de 1959, publicado en La Gaceta, Diario Oficial de la República de Honduras, con fecha 3 de julio de 1959 y nombrado mediante Resolución IHSS Nº01/20-01-2014 de fecha 20 de enero del 2014, de la Comisión Interventora del IHSS, conforme a las atribuciones otorgadas mediante Decreto Ejecutivo Nº PCM-011- 2014 de fecha 15 de Enero de 2014; publicado el 17 de enero de 2014 en la Gaceta, Diario Oficial de la Repúblicas, con Oficinas Administrativas en el Barrio Abajo de Tegucigalpa, con R.T.N. Nº08019003249605, quien para los efectos de este Contrato se denominará **"EL INSTITUTO"** y por otra parte xxxxx hondureño, mayor de edad, y de este domicilio con dirección en xxxxx, con número de celular, y correo electrónico, xxxxxxx actuando en su calidad de Gerente General y Representante Legal de la **SOCIEDAD_.**,según consta en poder de administración otorgado a su favor mediante Instrumento Público número del de de ante los oficio del notario; inscrito bajo el tomo, numero del Registro de la Propiedad Inmueble y Mercantil de ; RTN No en adelante denominado **"EL CONTRATISTA"**, hemos convenido en celebrar como en efecto celebramos, el presente **CONTRATO DEL SERVICIO DE** "**Adquisición de Solución de Comunicación Core Firewall Interno, Switches de Acceso, Certificación y Reparación de Fibra Óptica, Solución de Seguridad Perimetral de Próxima Generación, Solución de Comunicación de Telefonía IP para el IHSS". ……** el cual se regirá de acuerdo a las siguientes cláusulas: **PRIMERA: OBJETO DEL CONTRATO**; manifiesta "EL INSTITUTO" que mediante Resolución Nº del de de , la comisión interventora acepto la recomendación de adjudicación del "CONTRATO DEL SERVICIO DE **"Adquisición de Solución de Comunicación Core Firewall Interno, Switches de Acceso, Certificación y Reparación de Fibra Óptica, Solución de Seguridad Perimetral de Próxima Generación, Solución de Comunicación de Telefonía IP para el IHSS". , a la empresa xxxx**

_____Derivado de la Licitación Pública Nacional N°026/2018, lo siguiente: (describir el servicio) **SEGUNDA: VALOR DEL CONTRATO Y FORMA DE PAGO**; el valor del servicio a suministrar por "EL CONTRATISTA", identificados en la cláusula anterior, asciende a la suma de xxxxxxxx_ **LEMPIRAS EXACTOS (L_____)** para un gran total de los servicios desglosado así: xxx, xxxx

El valor todos los servicios a suministrar del contrato será pagado en Lempiras, con recursos propios disponibles por el periodo que corresponde al ejercicio fiscal 2018 y anteproyecto del presupuesto del año 2019, se harán pagos mensuales en moneda nacional (Lempiras). El proveedor Requerirá el pago al "INSTITUTO" y adjuntará a la solicitud el informe, copia de contrato y recibo a nombre de "INSTITUTO". **TERCERA: PRECIO A QUE SE SUJETA EL CONTRATO**; el precio o valor del contrato incluido en la Cláusula Segunda permanecerá fijo durante el período de validez del contrato y no será sujeto a variación alguna, solo en aquellos casos en que favorezcan al "INSTITUTO". **CUARTA: PLAZO DE EJECUCION**; conforme a lo establecido en la cláusula primera durante todos los días de los doce meses contratados el servicio se prestará en el porcentaje de disponibilidad solicitado, sin interrupción alguna y será supervisado por personal Gerencia de Tecnología de Información y Comunicación del Instituto de conformidad a lo establecido en las bases de licitación a partir de la orden de inicio; **QUINTA: GARANTIA DE CUMPLIMIENTO**; diez días hábiles después de la suscripción del contrato y con el objeto de asegurar al "EL INSTITUTO", el cumplimiento de todos los plazos, condiciones y obligaciones de cualquier tipo, especificadas o producto de este contrato, "EL CONTRATISTA" constituirá a favor de "EL INSTITUTO", una Garantía de Cumplimiento equivalente al quince por ciento (15%) del valor total de este contrato, vigente hasta tres (3) meses después del plazo previsto para la prestación del servicio para el año. La no presentación de la garantía solicitada en esta cláusula dará lugar a la resolución del contrato sin derivar responsabilidad alguna para "EL INSTITUTO". La garantía de cumplimiento será devuelta por "EL INSTITUTO", a más tardar dentro de los noventa (90) días calendario siguiente a la fecha en que "EL CONTRATISTA" haya cumplido con todas sus obligaciones contractuales. **SEXTA: CLAUSULA OBLIGATORIA DE LAS GARANTIAS**; todos los documentos de garantía deberán contener la siguiente cláusula obligatoria: **"LA PRESENTE GARANTÍA ES SOLIDARIA, INCONDICIONAL, IRREVOCABLE Y DE REALIZACIÓN AUTOMÁTICA, DEBIENDO SER EJECUTADA POR EL VALOR TOTAL DE LA MISMA, AL SIMPLE REQUERIMIENTO DEL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL (IHSS), ACOMPAÑADA DE LA RESOLUCIÓN ADMINISTRATIVA CORRESPONDIENTE, SIN NECESIDAD DE TRÁMITES PREVIOS AL MISMO. SIN PERJUICIO DE LOS AJUSTES QUE PUDIERAN HABER, SI FUERE EL CASO, QUE SE HARAN CON POSTERIORIDAD A LA ENTREGA DEL VALOR TOTAL. QUEDANDO ENTENDIDO QUE ES NULA CUALQUIER CLÁUSULA QUE CONTRAVENGA LO ANTERIOR. LA PRESENTE TENDRÁ CARÁCTER DE TÍTULO EJECUTIVO Y SU CUMPLIMIENTO SE EXIGIRÁ POR LA VÍA DE APREMIO. SOMETIÉNDOSE EXPRESAMENTE A LA JURISDICCIÓN Y COMPETENCIA DE LOS TRIBUNALES DEL DEPARTAMENTO DE FRANCISCO MORAZÁN."** A las garantías no deberán adicionarles cláusulas que anulen o limiten la cláusula obligatoria. **SEPTIMA: ERRORES Y OMISIONES EN LA OFERTA**; los errores contenidos en la oferta y otros documentos presentados por "EL CONTRATISTA" y

que se incorporen al contrato, correrán por cuenta y riesgo de este, independientemente de cualquiera de las garantías mencionadas en este contrato y sin perjuicio de cualquier otro derecho que "EL INSTITUTO", pueda tener o usar para remediar la falta; "**OCTAVA: CESION DEL CONTRATO O SUB-CONTRATACION**; Los derechos derivados de este contrato no podrán ser cedidos a terceros,. **NOVENA: CLAUSULA DE SANCION POR INCUMPLIMIENTO**; en caso de incumplimiento en la prestación de los servicios objeto del presente contrato descritos en la cláusula PRIMERA "EL CONTRATISTA" pagará a "EL INSTITUTO" en concepto de multa 0.36% del valor mensual. Si la falta de prestar el servicio no justificada diera lugar a que el total cobrado por la multa aquí establecida ascendiera al diez por ciento (10%) del valor total de este contrato "EL INSTITUTO", podrá considerar la resolución total del contrato y hacer efectiva la garantía de cumplimiento, sin incurrir por esto en ninguna responsabilidad de su parte, sin incurrir por esto en ninguna responsabilidad de su parte. "EL INSTITUTO" no pagará bonificación alguna por el cumplimiento del contrato antes de lo previsto. **DECIMA: RELACIONES LABORALES**; "EL CONTRATISTA" asume en forma directa y exclusiva, en su condición de patrono, todas las obligaciones laborales y de seguridad social con el personal que asigne a las labores para la prestación de servicio descritos en la cláusula primera, relacionado con el cumplimiento del presente contrato, relevando completamente a "EL INSTITUTO"," de toda responsabilidad al respecto, incluso en caso de accidente de trabajo o enfermedad profesional. **UNDECIMA: MODIFICACIÓN;** el presente Contrato podrá ser modificado dentro de los límites previstos en los Artículos 121, 122 y 123 de la Ley de Contratación del Estado, mediante la suscripción de un Adendum en las mismas condiciones que el presente contrato**. DUODECIMA: CAUSAS DE RESOLUCION DEL CONTRATO**; el grave o reiterado incumplimiento de las cláusulas convenidas, la falta de constitución de la garantía de cumplimiento del contrato o de las demás garantías a cargo del contratista dentro de los plazos correspondientes, la disolución de la sociedad mercantil contratista, la declaración de quiebra o de suspensión de pagos del contratista, o su comprobada incapacidad financiera, los motivos de interés público o las circunstancias imprevistas calificadas como caso fortuito o fuerza mayor, sobrevinientes a la celebración del contrato, que imposibiliten o agraven desproporcionadamente su ejecución, el incumplimiento de las obligaciones de pago más allá del plazo de cuatro (4) meses, el mutuo acuerdo de las partes, igual sucederá en caso de recorte presupuestarios de fondos nacionales que se efectúe por razón de la situación económica y financiera del país, la estimación de la percepción de ingresos menores a los gastos proyectados y en caso de necesidades imprevistas o de emergencia, lo anterior en cumplimiento del Artículo 69 del Decreto N°141-2017 que contiene el Presupuesto de Ingresos de La Administración Pública para el año 2018, publicado el 19 de enero de 2018, en la Gaceta Diario Oficial de la República, son causas de resolución de este contrato. **DECIMO TERCERA: FUERZA MAYOR O CASO FORTUITO;** Para los efectos del presente contrato se considera como caso fortuito o fuerza mayor debidamente justificados a juicio de "EL INSTITUTO", entre otras: catástrofes provocadas por fenómenos naturales, accidentales, huelgas, guerras, revoluciones, motines, desorden social, naufragio o incendio**. DECIMO CUARTA: VIGENCIA DEL CONTRATO**; El presente contrato entrará en vigencia a partir de su firma y emisión de su orden de inicio terminará por el cumplimiento normal de las prestaciones de las partes establecidas en este contrato que es doce (12) meses a partir de su firma. **DECIMO QUINTA: DOCUMENTOS INTEGRANTES DE ESTE CONTRATO**; forman parte de este CONTRATO: Los documentos de licitación constituidos por aviso de publicación, las bases de la Licitación Pública Nacional No 026/2018, incluyendo las aclaraciones a las mismas, emitidas por "EL CONTRATANTE" o remitidas por "EL

CONTRATISTA", la oferta técnica revisada, la oferta económica, así como cualquier otro documento que se anexa a este contrato por mutuo acuerdo de las partes. **DECIMO SEXTA: NORMAS SUPLETORIAS APLICABLES;** en lo no previsto en el presente contrato, serán aplicables las normas contenidas en la Ley de Contratación del Estado y su Reglamento, la Ley General de la Administración Pública, la Ley de Procedimiento Administrativo, la Ley Orgánica de Presupuesto y el Presupuesto General de Ingresos y Egresos de la República año 2018 y su Reglamento, demás leyes vigentes en Honduras que guardan relación con los procesos de contratación del Estado. Asimismo, en cumplimiento al Decreto N°141-2017 que contiene las Disposiciones Generales del Presupuesto General de Ingresos y Egresos de la República y de las Instituciones Descentralizadas, para el año 2018, se transcribe el **Artículo 69** del mismo que **textualmente indica**: "En todo contrato financiado con fondos externos, la suspensión o cancelación del préstamo o donación puede dar lugar a la rescisión o resolución del contrato, sin más obligación por parte del Estado, que el pago correspondiente a las obras o servicios ya ejecutados a la fecha de vigencia de la rescisión o resolución del contrato. Igual sucederá en caso de recorte presupuestario de fondos nacionales que se efectúe por razón de la situación económica y financiera del país, la estimación de la percepción de ingresos menor a los gastos proyectados y en caso de necesidades imprevistas o de emergencia. **Lo dispuesto en este Artículo debe estipularse obligatoriamente en todos los contratos que se celebren en el sector público.** En cumplimiento del numeral Primero del Acuerdo SE-037-2013 publicado el 23 de agosto de 2013, en el Diario Oficial La Gaceta**,** se establece **DECIMO SEPTIMA: "CLAUSULA DE INTEGRIDAD.-** Las partes en cumplimiento a lo establecido en el Artículo 7 de la Ley de Transparencia y Acceso a la Información Pública (LTYAIP) y con la convicción de que evitando las prácticas de corrupción podremos apoyar la consolidación de una cultura de transparencia, equidad y rendición de cuentas en los procesos de contratación y adquisiciones del Estado, para así fortalecer las bases del estado de derecho, nos comprometemos libre y voluntariamente a: 1. Mantener el más alto nivel de conducta ética, moral y de respeto a las leyes de la república, así como los valores: INTEGRIDAD, LEALTAD CONTRACTUAL, EQUIDAD, TOLERANCIA, IMPARCIALIDAD Y DISCRESION CON LA INFORMACION CONFIDENCIAL QUE MANEJAMOS, ABSTENIENDONOS A DAR INFORMACIONES PUBLICAS SOBRE LA MISMA, 2). Asumir una estricta observancia y aplicación de los principios fundamentales bajo los cuales se rigen los procesos de contratación y adquisiciones públicas establecidas en la Ley de Contratación del Estado, tales como transparencia, igualdad y libre competencia; 3) Que durante la ejecución del contrato ninguna persona que actúa debidamente autorizada en nuestro nombre y representación y que ningún empleado o trabajador, socio o asociado, autorizado o no realizará: a) Prácticas corruptivas, entendiendo éstas como aquellas en la que se ofrece dar, recibir, o solicitar directa o indirectamente, cualquier cosa de valor para influenciar las acciones de la otra parte; b) Prácticas Colusorias: entendiendo estas como aquellas en las que denoten sugieran o demuestren que existen un acuerdo malicioso entre dos o más partes o entre una de las partes, y uno y varios terceros, realizados con el propósito de alcanzar un propósito inadecuado, incluyendo influenciar de forma inapropiada las acciones de la otra parte; 4) Revisar y verificar toda la información que deba ser presentada a través de terceros, a la otra parte para efectos del contrato y dejamos manifestado que durante el proceso de contratación o adquisición causa de este contrato, la información intercambiada fue debidamente revisada y verificada por lo que ambas partes asumen y asumirán la responsabilidad por el suministro de información inconsistente , imprecisa o que no corresponda a la realidad, para efectos de este contrato; 5) Mantener la debida confidencialidad sobre toda la información a que se tenga acceso por razón del contrato, y no

proporcionarla ni divulgarla a terceros y a su vez, abstenernos de utilizarla para fines distintos; 6. Aceptar las consecuencias a que hubiere lugar, en caso de declararse el incumplimiento de alguno de los compromisos de esta Cláusula por Tribunal competente, y sin perjuicio de la responsabilidad civil o penal en la que se incurra; 7. Denunciar en forma oportuna ante las autoridades correspondientes cualquier hecho o acto irregular cometido por nuestros empleados o trabajadores, socios o asociados, del cual se tenga un indicio razonable y que pudiese ser constitutivo de responsabilidad civil y/o penal. Lo anterior se extiende a los subcontratistas con los cuales el Contratista o Consultor contrate, así como a los socios, asociados, ejecutivos y trabajadores de aquellos. El incumplimiento de cualquiera de los enunciados de esta cláusula dará lugar: a) De parte del Contratista o Consultor: i. A la inhabilitación para contratar con el Estado, sin perjuicio de las responsabilidades que pudieren deducírsele; ii) A la aplicación al trabajador ejecutivo representante, socio, asociado o apoderado que haya incumplido esta cláusula de las sanciones o medidas disciplinarias derivados del régimen laboral y, en su caso entablar las acciones legales que correspondan. B. De parte del Contratante: i. A la eliminación definitiva del Contratista o Consultor y a los subcontratistas responsables o que pudiendo hacerlo no denunciaron la irregularidad de su Registro de Proveedores y Contratistas que al efecto llevare para no ser sujeto de elegibilidad futura en procesos de contratación; ii. A la aplicación al empleado o funcionario infractor, de las sanciones que correspondan según el Código de Conducta Ética del Servidor Público, sin perjuicio de exigir la responsabilidad administrativa, civil y/o penal a las qué hubiere lugar. En fe de lo anterior, las partes manifiestan la aceptación de los compromisos adoptados en el presente documento bajo el entendido que esta Declaración forma parte integral del Contrato firmado voluntariamente para constancia.”. **DECIMO OCTAVA: JURISDICCION Y COMPETENCIA**; para la solución de cualquier situación controvertida derivada de este contrato y que no pudiera arreglarse conciliatoriamente, ambas partes se someten a la jurisdicción y competencia de los Juzgados del Municipio del Distrito Central. En fe de lo cual y para constancia, ambas partes suscribimos este contrato, en la Ciudad de Tegucigalpa, M.D.C., a los ---------- días del mes de ------- del año dos mil dieciocho.

Nota: Si así lo considerase el IHSS, éste modelo de contrato podrá ser ajustado al momento de definirse la Adjudicación

Dr. Richard Zablah	**XX**
Director Ejecutivo	**Representante Legal**

Aviso de Licitación Pública
República de Honduras
Instituto Hondureño de Seguridad Social (IHSS) Licitación Pública Nacional
LPN N° 026/2018

"Adquisición de Solución de Comunicación Core Firewall Interno, Switches de Acceso, Certificación y Reparación de Fibra Óptica, Solución de Seguridad Perimetral de Próxima Generación, Solución de Comunicación de Telefonía IP para el IHSS".

El Instituto Hondureño de Seguridad Social (IHSS) invita a las sociedades mercantiles interesadas en participar en la Licitación Pública Nacional N° LPN/026/2018 a presentar ofertas selladas para la "Adquisición de Solución de Comunicación Core Firewall Interno, Switches de Acceso, Certificación y Reparación de Fibra Óptica, Solución de Seguridad Perimetral de Próxima Generación, Solución de Comunicación de Telefonía IP para el IHSS". .

El financiamiento para la realización del presente proceso proviene exclusivamente de fondos propios del IHSS. La licitación se efectuará conforme a los procedimientos de Licitación Pública Nacional (LPN) establecidos en la Ley de Contratación del Estado y su Reglamento.

Los interesados podrán adquirir los documentos de la presente licitación, en la Subgerencia de Suministros Materiales y Compras ubicada en el Sexto Piso del Edificio Administrativo del Instituto Hondureño de Seguridad Social**,** Barrio Abajo, Tegucigalpa M.D.C. de 8:00 a.m. a 4:00 p.m. previo al pago de (L300.00) en la Tesorería del IHSS; a partir **del día 30 de octubre del 2018**. Los documentos de la licitación también podrán ser examinados en el Sistema de Información de Contratación y Adquisiciones del Estado de Honduras, "HonduCompras" (www.honducompras.gob.hn) y en el Portal de Transparencia del IHSS (www.ihss.hn).

Las ofertas deberán ser presentadas en la siguiente dirección: Lobby del IHSS, 1 piso del Edificio Administrativo, Barrio Abajo, Tegucigalpa, M.D.C. a más tardar a las 10:00 a.m. del **día 10 de diciembre de 2018** y ese mismo día a las 10:15 a. m. en el Auditorio del 11 piso se celebrará en audiencia pública la apertura de ofertas en presencia de los oferentes o de sus representantes legales o de la persona autorizada por el oferente que acredite su condición mediante carta, firmada por el representante legal de la sociedad mercantil. Las ofertas que se reciban fuera de plazo serán rechazadas. Todas las ofertas deberán estar acompañadas de una Garantía de Mantenimiento de la oferta por el 2% del monto de la oferta.

Tegucigalpa, M.D.C. octubre de 2018

Dr. Richard Zablah Asfura
Director Ejecutivo