



INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

MEMORANDO

No. 16893-GAYF-2021

PARA: **Abog. Vilma C. Morales**
Presidenta Comisión Interventora

DE: **Lic. Edwin Orlando Medina**
Gerente Administrativo y Financiero

ASUNTO: **Remisión de Actas**

FECHA: 8 de diciembre de 2021




Para aprobación se remite Memorando No. 4029-SGSMYC-2019 donde remiten documentación soporte Acta 4 Recomendación proceso de **Licitación Privada No. 017/2021 "Adquisición e Instalación de una Plataforma de alta Disponibilidad CLUTER CHECK PIN (2 NODOS) para el Instituto Hondureño de Seguridad Social (IHSS)".**

Se adjunta la siguiente información:

Acta N° 1 de Apertura de oferta
Acta N° 2 Evaluación de la Documentación Legal
Acta N° 3 Evaluación de la Documentación Técnica
Acta N° 4 Recomendación
Memorando N° 4029-SGSMYC-2021
Memorando N° 883-SGP/IHSS, Disponibilidad Presupuestaria.
Memorando No. -10472-GAYF-2021 autorizaciones proceso
Memorando N 1800 SGIMSG-2021-CNSH-GRSAS-2021
Certificación de Pliegos y Términos de Referencia CPC N C-0009-2021

Atentamente,

 Subgerencia de Suministros Materiales y Compras
Archivo

EOMC/Roxana

Ab
2021



INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

DOCUMENTO PARA OTORGAMIENTO DE VISTO BUENO

VISTO BUENO

C-0009-2021

Tegucigalpa, M.D.C.

A: **Abogada Vilma Cecilia Morales Montalván**
Presidenta Comisión Interventora
Instituto Hondureño de Seguridad Social

DE: **Edwin Orlando Medina Castro** - CPC número: **0062**

FECHA: 7 de diciembre de 2021

En seguimiento al proceso de Licitación Privada LP-017-2021 "ADQUISICION E INSTALACION DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK PINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL (IHSS), se informa lo siguiente:

1. Se otorga **Visto Bueno** al documento ACTA No.4 RECOMENDACIÓN DEL PROCESO LICITACION PRIVADA LP-017-2021 "ADQUISICION E INSTALACION DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK PINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL (IHSS)

Haciendo constar que la documentación de soporte que he tenido a la vista se ajusta al marco regulatorio y normativo pertinente a la contratación pública.

Este Visto Bueno no exime de ningún tipo de responsabilidad a los funcionarios y empleados que participaron en la elaboración y aprobación del documento al que se le otorga.

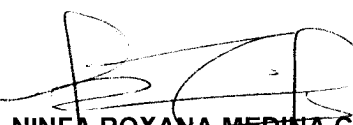
Firma: 
Nombre: **Edwin Orlando Medina Castro**
Número: **0062**




CERTIFICACIÓN

La infrascrita Jefe de la Unidad de Normas y Seguimiento y Delegada de la Comisión Interventora del INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL (IHSS), certifica los Dos (2) y Cinco (5) del punto de Agenda No.4 del Acta de Sesión Ordinaria No.697 donde se emite la **RESOLUCIÓN CI IHSS-GAYF No.1942/08-12-2021** de fecha 8 de diciembre de 2021, relacionada con las Actas del Proceso de Licitación Privada LP No.017-2021 "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL (IHSS)"; que en su parte conducente dice: "... **RESUELVE:**... **2.** Adjudicar el proceso de la Licitación Privada LP No.017-2021 "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL (IHSS)" a la empresa SISTEMAS EFICIENTES S.A. DE C.V. (SEFISA) por un monto de UN MILLON SETECIENTOS CUARENTA Y CINCO MIL LEMPIRAS EXACTOS (L1,745,000.00) ya que cumplió con la presentación de toda la Documentación Legal, Idoneidad Técnica, Financiera, especificaciones y condiciones técnicas y su oferta es aceptable conforme al presupuesto asignado por el IHSS para este proceso en mención... **5.** Instruir a la Gerencia Administrativa y Financiera para que proceda a remitir a la Oficina Normativa de Contratación y Adquisiciones del Estado (ONCAE) una copia electrónica de la Certificación C-0009-2021 de fecha 7 de diciembre de 2021 respectivamente, donde otorga Visto Bueno en su firma y sello, número correlativo y codificado por tipo de documento, a más tardar diez (10) días después de ser otorgada, en cumplimiento al Artículo 5 del Reglamento Operativo de Acreditación y Revocación de Certificación del Comprador Público Certificado. **6.** Transcribir los Resolutivos Dos (2) y Cinco (5) de la presente Resolución a la Gerencia Administrativa y Financiera para los efectos correspondientes con el fin de ser remitido a la Oficina Normativa de Contratación y Adquisiciones del Estado (ONCAE)... **F) VILMA C. MORALES M.,** Presidenta CI IHSS. **F) VILMA C. MORALES M.,** Presidenta CI IHSS. **F) ROBERTO CARLOS SALINAS,** Miembro CI IHSS. **F) GERMAN EDGARDO LEITZELAR V.,** Miembro CI IHSS. **F) NINFA ROXANA MEDINA CASTRO,** Jefe Unidad de Normas y Seguimiento IHSS y Delegada Comisión Interventora IHSS en Resolución CI IHSS No.797/24-11-2015".

Y para los fines correspondientes se extiende la presente en la ciudad de Tegucigalpa, Municipio Distrito Central, a los ocho días del mes de diciembre del año dos mil veintiuno.


NINFA ROXANA MEDINA CASTRO
Jefe Unidad de Normas y Seguimiento IHSS y Delegada
Comisión Interventora en Resolución CI IHSS No.797/24-11-2015



Roxana
9/12/2021



INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

MEMORANDO N° 4029-SGSMYC- 2021

PARA: Lic. Edwin Orlando Medina Castro
Gerencia Administrativa y Financiera

DE: Lic. Hector Joel Figueroa Hernandez
Encargado de la Subgerencia de Suministros

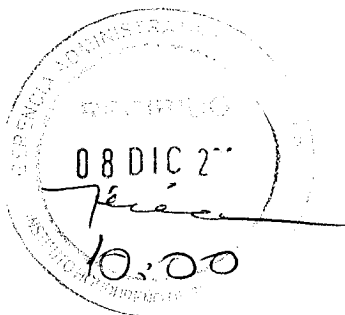
ASUNTO: VISTO BUENO LP 017-2021

FECHA: lunes 06 de diciembre de 2021

Adjunto al presente se remite documentación soporte del proceso, ACTA N°4 RECOMENDACIÓN DEL PROCESO LICITACION PRIVADA LP-017-2021 "ADQUISISION E INSTALACION DE UNA PALTAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK PIN (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL (IHSS), con su respectivo **Comprador Publico Certificado** N° C-0009-2021 de fecha 07 de Diciembre del presente año.

Atentamente,

CC: Archivo
HJF/BES



Subgerencia de Suministros, Materiales y Compras, Edificio Administrativo del IHSS

Teléfonos: (504) 2222-6922, Ext. 2114, 5211 y 1305

www.ihss.hn



**INSTITUTO HONDUREÑO DE SEGURIDAD
SOCIAL**

MEMORANDO N° 001-CE-LP-017/2021

Para: **Lic. Hector Figueroa**
Encargado de la Subgerencia de Suministros Materiales y Compras

De: **Ing. David Ardino**
Comisión Evaluadora



Asunto: **Remisión de Actas**

Fecha: Martes 09 de diciembre de 2020

Por este medio, se le remite para su consideración y aprobación por parte de la Comisión Interventora del IHSS las Actas; del proceso de la LICITACION PRIVADA N° LP-017-2021 "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL IHSS".

Se anexan

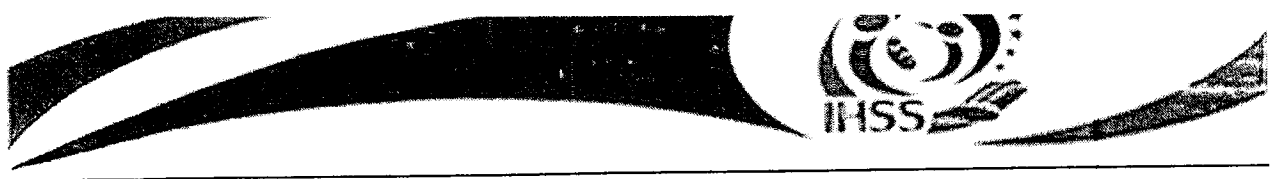
- 1) Acta No 1 Recepción y Apertura de Ofertas ✓
- 2) Acta No 2 Evaluación de la Documentación Legal y Especificaciones Técnicas ✓
- 3) Acta No 3 Evaluación de las Especificaciones Técnicas ✓
- 4) Acta No 4 Recomendación ✓
- 5) Memorando No 1800-GTIC-IHSS-2021 Solicitud de Autorización del Proceso ✓
- 6) Memorando No 10472-GAyF-2021 ✓
- 7) Memorando No 883-SGP/IHSS -2021 ✓

Atentamente,

 **Expediente LP/017/2021**

HF/DA

Amorlen
SUBGERENCIA DE SUMINISTROS MATERIALES Y COMPRAS
TEL: 2222-6922
WWW.IHSS.HN



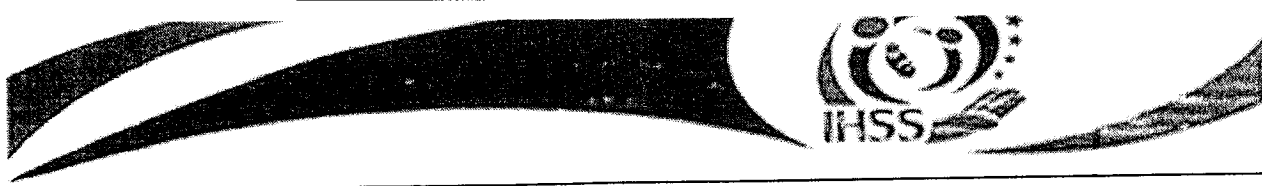
ACTA N° 4

RECOMENDACIÓN LICITACION PRIVADA N° LP-017-2021 "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL IHSS".

En la ciudad de Tegucigalpa, Municipio del Distrito Central, a los tres días (03) días del mes de diciembre del año dos mil veintiuno (2021) siendo las nueve de la mañana (9:00 a.m.), reunidos en las oficinas de la Subgerencia de Suministros Materiales y Compras, del Instituto Hondureño de Seguridad Social, ubicada en el sexto piso del Edificio Administrativo, Barrio Abajo, Tegucigalpa M.D.C. los miembros de la Comisión de Evaluación de la LICITACION PRIVADA N° LP-017-2021 "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL IHSS"., Abogada Belki Erazo, Representante de la Unidad de Asesoría Legal, Ingeniero David Andino, Representante de la Subgerencia de Suministros Materiales y Compras, Licda. Yohana Vanessa Reconco, Representante de la Gerencia Administrativa y Financiera, Ingenieros Francisco Franco y Jorge Echenique Representante de la Gerencia de Tecnología de Información y Comunicaciones, con el objeto de Realizar la Recomendación sobre la oferta presentada en este proceso de licitación anteriormente descrito que fue iniciado el día viernes 29 de octubre de 2021 por lo que se procede de la siguiente manera: **PRIMERO:** Se informa que mediante Resolución CI IHSS-GAYF N° 1630/04-10-2021 de fecha 04 de octubre del año 2021, se aprobaron las bases de la LICITACION PRIVADA N° LP-017-2021 "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL IHSS". **SEGUNDO:** Se informa que para este proceso de Licitación Privada N° LP-017-2021 se invitaron a las siguientes empresas: 1. Sistemas Eficientes (SEFISA), Oficio No 960-DEI-IHSS-2021. 2.- Componentes El Orbe, Oficio No 960-DEI-IHSS-2021. **TERCERO:** Se procedió a revisar la documentación de la oferta económica presentada por la única empresa participante: Sistemas Eficientes S.A. de C.V. (SEFISA), presenta una oferta económica, por un monto de Un millón, Setecientos Cuarenta y Cinco Mil Lempiras Exactos (L.1,745,000.00) presentando una garantía bancaria de mantenimiento de oferta No. 2413221, extendida por Banco Ficohsa, por un monto de Treinta y Cuatro Mil Lempiras Exactos (L.34,900.00), con una vigencia del 29 de octubre de 2021 hasta el 26 de febrero del año 2022. **CUARTO:** Se hace énfasis que la Disponibilidad Presupuestaria para la "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL IHSS" es por el valor de Seis Millones Cuatrocientos Cincuenta y Cuatro Mil Cuatrocientos Cincuenta y Dos Lempiras Exactos (L 6,454,452.00), la estructura presupuestaria que se detalla a continuación:

Fondo	ACCE Actividades Centrales
Área Funcional	AC 190004 Actividades Centrales
Centro Gestor	AC 217000 Gerencia de Tecnología Información y Comunicación
Pospre	39300 Útiles y Materiales Eléctricos
Pospre	42120 Equipos varios de oficina
Pospre	42600 Equipos para Computación
Pospre	47110 Construcciones y Mejoras de Bienes
Monto Disponible	L 6,454,452.00

Según consta en el memorando No 883-SGP/IHSS-2021 de fecha 16 de abril de 2021, firmado por el Licenciado José Lorenzo Cotc, Subgerente de Presupuesto. **QUINTO:** La Comisión Evaluadora elaboró el Acta N°2, EVALUACIÓN DE LA DOCUMENTACION LEGAL Y DE LA DOCUMENTACION DE LAS CONDICIONES Y ESPECIFICACIONES TECNICAS de fecha diez (10) del mes de noviembre del año dos mil veintiuno (2021) y de conformidad a la Sección SECCION I - INSTRUCCIONES A LICITANTES, IO-09 DOCUMENTOS A PRESENTAR de las Bases de Licitación Privada No LP 017-2021, luego de revisar, analizar y evaluar, la documentación legal solicitada, se concluyó que La Empresa Sistemas Eficientes S.A. de C.V. (SEFISA), cumplió con toda la documentación legal solicitada en las Bases de Licitación, por consiguiente la oferta presentada por esta empresa, pasa a la evaluación técnica. **SEXTO:** Seguidamente los integrantes de la Comisión Evaluadora de esta licitación en un acuerdo establecen que los miembros técnicos Ing. Francisco Franco e Ing. Jorge Echenique, Representación de la Gerencia de Tecnología de Información y Comunicación, revisen, analicen y evalúen, la documentación, especificaciones y condiciones técnicas solicitadas en las bases de Licitación Privada Nacional LP 017-2021, concluyendo que la empresa Sistemas Eficientes S.A. de C



(SEFISA), cumple con las especificaciones técnicas solicitadas en las bases de licitación, según conste en el Acta de Evaluación Técnica de fecha 18 días del mes de noviembre de 2021, por lo que la oferta presentada por esta empresa puede pasar a la siguiente etapa de evaluación económica. **SEPTIMO:** Los miembros de la Comisión Evaluadora de esta Licitación en común acuerdo establecieron que la Licda. Yohana Vanessa Reconco, Representante de la Gerencia Administrativa y Financiera e Ingeniero David Andino, Representante de la Subgerencia de Suministros Materiales y Compras, realizaron la comparación y Evaluación Económica del precio presentado por la empresa Sistemas Eficientes S.A. de C.V. (SEFISA), que superó la Evaluación Legal y Técnica, por lo que se realizó el análisis económico y del precio ofertado por este oferente y se comparó con la disponibilidad que cuenta el Instituto para la "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL IHSS" ilustrando como resultado lo siguiente:

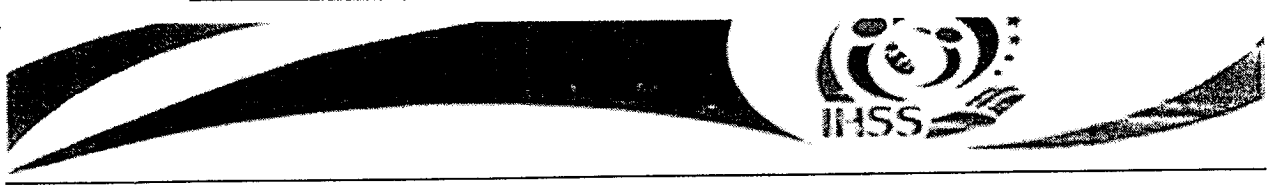
Empresa Oferente	Descripción del Bien	Oferta Presentada	Presupuesto del IHSS
Sistemas Eficientes S.A. de C.V. (SEFISA)	"Adquisición e Instalación de una Plataforma de alta Disponibilidad Cluster Check Point (2 nodos) para el Instituto Hondureño de Seguridad Social IHSS"	L 1,745,000.00	L 6,454,452.00

Concluyendo que existe la asignación presupuestaria para la "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL IHSS". **OCTAVO:** Considerando todo anteriormente descrito, la empresa oferente Sistemas Eficientes S.A. de C.V. (SEFISA), cumplió con la presentación de toda la Documentación Legal, Idoneidad Técnica, Financiera, especificaciones técnicas y presenta oferta aceptable conforme al presupuesto asignado por el IHSS, según el análisis económico realizado que consta en el considerando anterior, por lo que la Comisión Evaluadora **RECOMIENDA:** A la Comisión Interventora del Instituto Hondureño de Seguridad Social (IHSS), **ADJUDIQUE:** LA LICITACION PRIVADA N° LP-017-2021 "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL IHSS", a la empresa Sistemas Eficientes S.A. de C.V. (SEFISA), por un monto total de UN MILLON SETECIENTOS CUARENTA Y CINCO MIL LEMPTRAS EXACTOS (L 1,745,000.00). La presente recomendación se fundamenta en los artículos 5, 11, 12, 32, 33, 38 numeral 2, 50, 51, 52, 55 y 57 de la Ley de Contratación del Estado y los artículos 11, 20, 37, 39, 51, 53, 110, 125, 132, 133, 135, 136, 139, 140 del Reglamento de la Ley de Contratación del Estado, Artículo 100 de la Ley para Optimizar la Administración Pública, Mejorar los Servicios a la Ciudadanía y Fortalecimiento de la Transparencia en el Gobierno y en la Parte II Condiciones Generales. No habiendo más que tratar se cerró la reunión de evaluación de la LICITACION PRIVADA N° LP-017-2021 "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL IHSS" Para constancia firmamos los abajo descritos la presente acta en la ciudad de Tegucigalpa, Municipio del Distrito Central siendo las once de la mañana (11:00 a.m.).

Abog. Belkis Erazo
Rep. Unidad de Asesoría Legal

Ing. David Andino.
Rep. Subgerencia de Suministros Materiales y Compras

Licda. Yohana Vanessa Reconco
Rep. Gerencia Administrativa y Financiera



Ing. Francisco Franco
Representantes de la Gerencia de Tecnología, Información y Comunicaciones

Ing. Jorge Echenique



INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

ACTA DE EVALUACIÓN TÉCNICA

EVALUACIÓN DE LA DOCUMENTACIÓN, CONDICIONES Y ESPECIFICACIONES TÉCNICAS DEL PROCESO LICITACIÓN PRIVADO NO. LPN 017-2021 “ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL (IHSS)”

En la Ciudad de Tegucigalpa, Municipio del Distrito Central, a los dieciocho días del mes de noviembre del año dos mil veintiuno, siendo las nueve de la mañana (9:00 a.m.), reunidos en las oficinas de la Subgerencia de Suministros, Materiales y Compras del Instituto Hondureño de Seguridad Social, ubicado en el sexto piso del Edificio Administrativo, Barrio Abajo, Tegucigalpa M.D.C, los miembros de la Comisión de Evaluación del **PROCESO LICITACIÓN PRIVADA No. LPN 017-2021 “ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL (IHSS)”**; integrada por el Ingeniero Francisco Alejandro Franco y el Ingeniero Jorge Arturo Echenique, representantes de la Gerencia de Tecnologías de Información y Comunicaciones, con el objeto de revisar, analizar y evaluar, la documentación, especificaciones y condiciones técnicas solicitadas en la Sección VI. Lista de Requisitos, 3. Especificaciones Técnicas. así: **PRIMERO**. Se inició con la revisión de las especificaciones Técnicas Mínimas solicitadas en las bases de la LICITACIÓN PRIVADA No. LPN 017-2021, de la empresa que califico para ser evaluadas técnicamente siendo esta SISTEMAS EFICIENTES S.A. DE C.V. (SEFISA). cómo se detalla en los siguientes cuadros de evaluación y cumplimiento:

EVALUACIÓN TÉCNICA

El Instituto Hondureño de Seguridad Social (IHSS), requiere la adquisición e instalación y servicios conexos para la implementación de una plataforma de alta disponibilidad para el perímetro Clúster Check Point (2 Nodos), utilizando la Infraestructura que ya ha adquirido el IHSS marca Check Point.

Debido a que el oferente presentó varios documentos que incluyen información técnica, económica, legal y manuales de uso, se utilizarán las siguientes abreviaturas para referirse a ellos, a continuación, se detalla:

- **ET:** Especificaciones técnicas
- **RT:** Respuesta técnica
- **DEF:** Documentación Económica/Financiera

Gerencia de Tecnología de Información y Comunicación
8 piso, Edificio Administrativo, Tegucigalpa
Teléfono: (504) 2237-4840, consultas@ihss.hn
www.ihss.hn


1



INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

DESCRIPCIÓN	SISTEMAS EFICIENTES S.A. (SEFISA)			
	CUMPLE		FOLIO	OBSERVACIÓN
	SI	NO		
Condiciones Técnicas				
1. Especificaciones Generales				
1. Se requiere un ClústerXL de Check Point el cual debe estar constituido por dos (2) equipos en modo activo/pasivo para la seguridad perimetral, brindando alta disponibilidad al IHSS.	X		ET 27	La oferta contempla los dos (2) equipos para la configuración en modo activo/pasivo como se solicita.
2. El proveedor deberá brindar los equipos y el software para la creación del Clúster como proyecto llave en mano para el IHSS.	X		ET 27	
3. El proveedor deberá hacerse cargo de la instalación, migración, configuración y soporte de los equipos nuevos y de los equipos que posee el IHSS marca Check Point.	X		ET 27	
4. El proveedor deberá incluir todos los accesorios, medios, equipos, etc. que sean necesarios para la puesta en producción de la solución a adquirir.	X		ET 27	
5. El oferente deberá brindar el licenciamiento de Software Check Point para los equipos solicitados.	X		ET 27	
6. Servicios de Capacitación por parte del representante del fabricante en el uso, administración, configuración y monitoreo de la solución adquirida para el Departamento de Infraestructura de la Gerencia de TIC del IHSS, para diez (10) personas como mínimo.	X		ET 27	
7. Servicio de garantía del fabricante, para los equipos, todos los componentes de hardware y software deben de tener una garantía de un (1) año como mínimo.	X		ET 27, 28	
8. Servicios de Suscripción con el Fabricante por un (1) 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	X		ET 28	



técnico (local y remoto cuando fuera necesario), actualizaciones y corrección de errores.				
9. Los equipos ofertados deben estar certificados por Check Point Software Technologies Ltd. para asegurar el funcionamiento correcto del software. Los oferentes deben entregar una constancia emitida por el fabricante de la solución donde se indique que los equipos están certificados para brindar los servicios requeridos por el IHSS.	X		ET 28	Subsanar SEFISA: No se incluye Certificación por parte de Check Point, que certifique que los equipos ofertados son compatibles con el Software Check Point. Respuesta SEFISA: En fecha 18 de noviembre de 2021, remite oficio donde anexa Carta enviada por el fabricante, donde Certifica que los Servidores Ofertados son compatibles con el Software Check Point.
10. La solución de software debe ser compatible con la Solución de Administración Check Point que posee el Instituto.	X		ET 28	
2. Características de la Solución				
11. La solución debe incluir las siguientes características: <ul style="list-style-type: none">• Modulo Firewall• Módulo de Prevención de Intrusión (IPS)• Adquisición de Identidad de Usuario• Módulo de Control de Aplicaciones• Módulo de Filtrado WEB• Modulo Anti-Bot• Modulo Antivirus / Antimalware• Emulación y Extracción de Amenazas• IPSec VPN	X		ET 3, 4 RT 1	



12. El Clúster debe estar conformado por dos (2) servidores. (Ver tabla de Especificaciones de Hardware (Clúster)).	X		ET 4 RT 1	
13. La solución debe tener la posibilidad de soportar la configuración y funcionalidad de Alta Disponibilidad (HA), la compartición de carga con sincronización de estado en sus modos de operación (Activo-Activo o Activo-Pasivo).	X		ET 4 RT 1	
14. Capacidad de distribuir las cargas de trabajo con al menos 3 conexiones a internet con diferentes ISPs, configurable ya sea manual o automática, en modo activo/pasivo o activo/activo.	X		ET 4 RT 1	Subsanar SEFISA: Certificar que el Clúster Soporta hasta 3 Conexiones de distintos ISP. Respuesta SEFISA: En fecha 18 de noviembre de 2021, remite oficio donde confirma con documentación del fabricante, que el equipo puede soportar 3 conexiones con diferente ISP.
15. 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. Los archivos de copias de seguridad pueden ser almacenados localmente y/o en un equipo remoto.	X		ET 4 RT 3, 4	
16. Los dispositivos de hardware sobre el que deberá ejecutarse la solución de seguridad perimetral deberán estar certificados por parte del fabricante de la solución, garantizado del correcto funcionamiento del software.	X		ET 4 RT 3, 4	



INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

17. Los equipos deben ser instalados en rack estándar (el oferente debe incluir los accesorios de instalación).	X		ET 5	
3. Características del Clúster				
18. El clúster deberá permitir una conmutación de falla transparente con pocas pérdidas o ninguna pérdida de paquetes.	X		ET 5	El protocolo de conmutación de Check Point permite la continuidad del tráfico, teniendo solo la pérdida de 1 a 2 paquetes durante la conmutación.
19. Debe tener un protocolo de clúster propietario de la marca.	X		ET 5 RT 6	
20. Debe permitir balanceo de carga en caso de ser necesario.	X		ET 5 RT 6	
21. El licenciamiento para el clúster deberá estar incluido en la solución.	X		ET 5	
22. Capacidad de lidiar con conexiones de tráfico asimétrico y corregir el mismo.	X		ET 5 RT 7	
23. Capacidad de listar el estado del clúster y de cada miembro de acuerdo con sus problemas.	X		ET 6 RT 8	<p>Subsanar SEFISA: La solución cuenta con algún monitoreo gráfico (Web o Aplicación), para visualizar el estatus del Clúster.</p> <p>Respuesta SEFISA: En fecha 18 de noviembre de 2015</p>



INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

				2021, remite oficio donde confirma que la solución posee una herramienta para el monitoreo grafico del Cluster.
24. Capacidad de utilizar IP virtualizada por el clúster para evitar problemas en el enrutamiento del tráfico al no depender de una interfaz física de los equipos.	X		ET 6 RT 9	
25. Capacidad de utilizar dirección MAC virtual para evitar problemas en las tablas de ARP después de la caída de uno de los miembros y que el tráfico sea continuo.	X		ET 6 RT 9	
26. Capacidad de manejar las conexiones por medio de un solo miembro.	X		ET 6 RT 10	
27. Sincronización de equipos mediante protocolo propietario e interfaz dedicada.	X		ET 6 RT 6	El equipo tiene la capacidad de configurar una red de sincronización, esta se configura en una interfaz dedicada para la sincronización.
28. Se debe poder definir un equipo con mayor prioridad para dejar el mismo como primario en caso de cualquier eventualidad y que este pueda ser el equipo siempre activo cuando se encuentre disponible.	X		ET 6 RT 10	
29. Permitir configurar las interfaces en modo monitoreo o no monitoreo.	X		ET 6 RT 11	
30. Capacidad de configuración de topología desde consola centralizada.	X		ET 7	6

Gerencia de Tecnología de Información y Comunicación

8 piso, Edificio Administrativo, Tegucigalpa

Teléfono: (504) 2237-4840, consultas@ihss.hn

www.ihss.hn



INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

				2021, remite oficio donde confirma que la solución posee una herramienta para el monitoreo grafico del Cluster.
24. Capacidad de utilizar IP virtualizada por el clúster para evitar problemas en el enrutamiento del tráfico al no depender de una interfaz física de los equipos.	X		ET 6 RT 9	
25. Capacidad de utilizar dirección MAC virtual para evitar problemas en las tablas de ARP después de la caída de uno de los miembros y que el tráfico sea continuo.	X		ET 6 RT 9	
26. Capacidad de manejar las conexiones por medio de un solo miembro.	X		ET 6 RT 10	
27. Sincronización de equipos mediante protocolo propietario e interfaz dedicada.	X		ET 6 RT 6	El equipo tiene la capacidad de configurar una red de sincronización, esta se configura en una interfaz dedicada para la sincronización.
28. Se debe poder definir un equipo con mayor prioridad para dejar el mismo como primario en caso de cualquier eventualidad y que este pueda ser el equipo siempre activo cuando se encuentre disponible.	X		ET 6 RT 10	
29. Permitir configurar las interfaces en modo monitoreo o no monitoreo.	X		ET 6 RT 11	
30. Capacidad de configuración de topología desde consola centralizada.	X		ET 7	6

Gerencia de Tecnologia de Informacion y Comunicaci3n

8 plso, Edificio Administrativo, Tegucigalpa

Tel3fono: (504) 2237-4840, consultas@ihss.hn

www.ihss.hn



			RT 11	
31. Capacidad de brindar redundancia de VPN sitio a sitio y VPN de acceso remoto con los equipos en alta disponibilidad.	X		ET 7 RT 12	
32. Licenciamiento se debe realizarse por Cores permitiendo crecimiento en cuanto a Cores cuando la Institución lo requiera.	X		ET 7 RT 12	
4. Rendimiento de Red				
33. 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.	X		ET 7- 8	Subsanar SEFISA: Presentar documentación del fabricante que acredite el cumplimiento de este ítem. Respuesta SEFISA: En fecha 18 de noviembre de 2021, remite oficio donde confirma que los servidores ofertada soporta el tráfico de red requerido por el IHSS.
34. Throughput de Firewall: El throughput de Firewall debe ser de al menos 30 Gbps en condiciones de producción.				
35. NGFW Throughput: 3 Gbps en condiciones de producción, teniendo activados los módulos de Control de Aplicaciones, IPS y el Firewall.				
36. Conexiones Concurrentes: Debe soportar al menos 3 millones de conexiones concurrentes.				
5. Solución de Firewall				
37. El módulo 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.	X		ET 8 RT 13	
38. El módulo 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,	X		ET 8- 9	7



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.			RT 13	
39. Debe permitir crear controles de acceso a por lo menos 150 aplicaciones/servicios/protocolos predefinidos.	X		ET 9 RT 14	
40. 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.	X		ET 9 RT 15	
41. 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.	X		ET 9 RT 15	
42. 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.	X		ET 9 RT 15	
43. El firewall debe soportar varios métodos de autenticación, al menos por usuario, por un cliente (a través de la dirección IP) y por sesión.	X		ET 9 RT 16	
44. El firewall debe permitir conectarse en modo transparente (bridge Mode).	X		ET 9 RT 16	
45. Debe soportar Bootp/DHCP Relay.	X		ET 9 RT 17	



46. Debe soportar sumarización de rutas (route aggregation) y redistribución de rutas a otros protocolos (route redistribution).	X		ET 10	
			RT 18- 19	
47. Debe soportar ruteo dinámico con RIP versión 2, OSPFv2, y BGP versión 4. Estos 3 protocolos deben ser soportados también en IPv6.	X		ET 10	
			RT 21	
48. Debe soportar control de ancho de banda basado en prioridades de pesos.	X		ET 10	
			RT 21	
49. Debe soportar servicios diferenciados integrados (DiffServ).	X		ET 10	
			RT 22	
50. Debe tener mecanismos de detección de engaños de IP, donde paquetes externos a la red usan direcciones internas para saltarse los controles de seguridad.	X		ET 10	
			RT 22- 23	
51. La consola de administración también debe permitir monitorear el estado de la alta disponibilidad.	X		ET 10	
			RT 23	
6. Módulo de Prevención de Intrusión (IPS)				
52. El módulo 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	X		ET 10	



basados en los contenidos del tráfico, en lugar de direcciones IP o puertos.				
53. 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. Debe proveer cobertura de protecciones para amenazas de clientes, servidores, sistemas operativos, infecciones de malware y gusanos.	X		ET 10- 11 RT 24- 25	
54. El IPS debe tener un software basado en el mecanismo de Fail Open.	X		ET 11 RT 26	
55. El IPS debe ofrecer un mecanismo automatizado para activar o administrar nuevas firmas a partir de las actualizaciones.	X		ET 11 RT 26	
56. El IPS debe poder inspeccionar el tráfico SSL	X		ET 11 RT 27	
57. El IPS debe soportar la configuración de excepciones basadas en la fuente, destino, servicio o una combinación de los tres.	X		ET 11 RT 28	
58. El módulo de IPS debe tener un mecanismo de correlación y reporte centralizado de eventos.	X		ET 11	10



			RT 29	
59. Debe soportar software configurable para realizar bypass en caso de alta carga, para garantizar rendimiento de red.	X		ET 11 RT 29	
60. Debe tener protección contra ataques DoS	X		ET 12 RT 30	
61. 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.	X		ET 12 RT 30	
62. El IPS debe ser capaz de realizar captura del paquete para protecciones específicas.	X		ET 12 RT 31	
63. 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.	X		ET 12 RT 32	
64. El administrador debe ser capaz de definir las exclusiones de redes y host de la inspección del IPS.	X		ET 12 RT 28	
65. La solución debe proteger del Envenenamiento de Caché DNS y prevenir a los usuarios el acceso a direcciones de dominio bloqueadas.	X		ET 12 RT 32	



66. 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.	X		ET 12	
			RT 34	
67. La solución debe cumplir la ejecución del protocolo Citrix.	X		ET 12	
			RT 34	
68. La solución debe permitir al administrador bloquear fácilmente el tráfico de entrada y/o de salida.	X		ET 12	
			RT 35	
69. Debe soportar Inspección de tráfico encriptado HTTPS tanto Inbound como Outbound. Sin necesidad de HW dedicado externo.	X		ET 12	
			RT 27	
70. Debe permitir la creación de excepciones a partir de los eventos reportados.	X		ET 13	
			RT 28	
71. El IPS integrado, debe incluir la habilidad de detener temporalmente la inspección y bloqueo en el Gateway, para efectos de "Troubleshooting".	X		ET 13	
			RT 36	
72. Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos. El administrador debe poder definir objetos de red y servicios a excluir.	X		ET 13	
			RT 36	
73. Debe soportar y proteger protocolos de VoIP (H.323, SIP, MGP y SCCP), asegurando que todos los paquetes de VoIP son estructuralmente válidos.	X		ET 13	



			RT 37
74. Debe permitir bloquear tráfico entrante, saliente o ambos correspondientes a determinados países, sin necesidad de actualizar manualmente los rangos IP correspondientes a cada país.	X		ET 13 RT 37
75. 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.	X		ET 13 RT 38
76. 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.	X		ET 13 RT 24- 25
77. Debe ser capaz de realizar captura de tráfico para análisis forense.	X		ET 13 RT 32

7. Adquisición de Identidad de Usuario

78. 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.	X		ET 14
79. 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.	X		ET 14 RT 39
80. La solución debe proteger a los clientes de ataques IP-spoofing y Identity-Spoofing.	X		ET 14





			RT 23	
81. Debe soportar el uso de varios esquemas de autenticación, como ser tokens, TACACS, RADIUS, certificados digitales.	X		ET 14 RT 40	
82. La solución debe soportar el uso de grupos alojados de LDAP.	X		ET 14 RT 41	
83. Con la finalidad de crear reglas de acceso por usuarios o grupos, debe poder integrarse con otras soluciones como: control de aplicaciones y filtrado de URL o filtrado de contenido.	X		ET 14 RT 22	
84. La solución debe retener la identidad de los usuarios aun cuando estos cambien la dirección IP del equipo cliente.	X		ET 14 RT 22	
85. La autenticación de los clientes y/o usuarios puede ser a través de sistemas operativos Windows, Linux, Mac OS, etc.	X		ET 14 RT 39	
8. Módulo de Control de Aplicaciones				
86. 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.	X		ET 14	
87. La solución debe contar con una base de datos de más de 6,000 aplicaciones diferentes y más de 250,000 widgets web	X		ET 15 RT	



INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

2.0 como mensajería instantánea, redes sociales video streaming, VoIP, juegos, entre otros.			42	
88. 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.	X		ET 15 RT 15, 42	
89. Debe inspeccionar el tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo SSL.	X		ET 15 RT 42	
90. Debe tener un servicio de clasificación basando en la nube que permita categorizar dinámicamente el tráfico Web.	X		ET 15 RT 43	
91. 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.	X		ET 15 RT 22, 41	
92. La solución debe ofrecer un mecanismo para limitar el uso de las aplicaciones basado en el consumo del ancho de banda.	X		ET 15 RT 22	
93. 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.	X		ET 15 RT 44	
94. Capacidad para identificar, 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.	X		ET 15 RT 42	



95. 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.	X		ET 15 RT 44	
96. 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.	X		ET 16 RT 45	
97. Debe tener la capacidad de prevenir infecciones de malware provenientes de aplicaciones y widgets de redes sociales.	X		ET 16 RT 45	
9. Módulo de Filtrado Web				
98. El Módulo 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.	X		ET 16	
99. 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, entre otros.	X		ET 16 RT 42	
100. El Módulo de Filtrado WEB deberá de poder aplicar seguridad SafeSearch a los motores de búsqueda.	X		ET 16 RT 46	
101. El Módulo de Filtrado WEB debe tener la capacidad de bloquear granularmente sitios basado en Web 2.0.	X		ET 16	



			RT 46	
102. La solución debe ser capaz de configurar reglas de filtrado con múltiples categorías.	X		ET 16 RT 42	
103. La solución debe ser capaz de crear un filtrado para un único sitio a ser soportado por múltiples categorías.	X		ET 16 RT 46	
104. La solución debe tener granularidad de los usuarios y grupos con las normas de seguridad.	X		ET 17 RT 47	
105. La solución debe permitir las excepciones de red basadas en los objetos de red definidos.	X		ET 17 RT 47	
106. La solución debe ofrecer un mecanismo de invalidez en la categorización para la base de datos de la URL.	X		ET 17 RT 47	
107. Debe inspeccionar el tráfico HTTPS, con el fin de prevenir riesgos de seguridad relacionados con el protocolo SSL.	X		ET 17	La solución ofertada ofrece la validación del URL en caso de presentar problemas la misma notificara.
108. 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).	X		ET 17 RT 48	



109. 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.	X		ET 17 RT 45	
110. El módulo de Filtrado WEB deberá tener la capacidad de filtrar páginas traducidas y en cache.	X		ET 17 RT 42	
111. El módulo 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.	X		ET 17 RT 47- 49	
112. 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.	X		ET 17 RT 49	
10. Módulo Anti-bot				
113. 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.	X		ET 18	
114. La solución debe poder detectar hosts internos infectados con botnets, analizando el tráfico de la red utilizando una tecnología multicapa.	X		ET 18 RT 49	
115. 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.	X		ET 18 RT 49	



116. 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.	X		ET 18	RT 50
117. La herramienta contra botnets deberá prevenir daños de robo de información mediante el bloqueo de las comunicaciones de las maquinas infectadas.	X		ET 18	RT 50
118. Debe incluir al menos 2000 patrones de comunicación de botnets.	X		ET 18	RT 51
119. La solución debe incluir al menos los siguientes métodos de identificación: a) Identificación de DNS de Command and control utilizadas por los criminales para controlar los bots. b) Identificación de patrones de comunicación utilizada por cada familia de bots.	X		ET 18	RT 50- 51
120. La solución debe utilizar tecnología de inspección multicapas.	X		ET 18	RT 51

11. Modulo Antivirus/Antimalware

121. 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 rogeware.	X		ET 19	RT 51
---	---	--	----------	----------



INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

122. El motor de inspección debe ser basado en firmas y análisis de comportamiento.	X		ET 19	
			RT 51	
123. 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.	X		ET 19	
			RT 52	
124. 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.	X		ET 19	
			RT 52	
125. El módulo de Antivirus / Antimalware debe hacer escaneo en tiempo real tanto de antivirus como de antimalware.	X		ET 19	
			RT 52	
126. Deberá basarse en patrones previniendo contra software espía y gusanos.	X		ET 19	
			RT 51	
127. 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.	X		ET 19	
			RT 53	
128. 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.	X		ET 19	
			RT 54	



129. Descompresión de archivos, con la opción de poder configurar el máximo nivel de anidación y de compresión para evitar ataques DoS.	X		ET 20	
			RT 54	
130. Debe soportar remover contenido malicioso de distintas partes de un documento, como mínimo: macros, objetos y archivos embebidos; y accesos URLs (links) a sitios externos.	X		ET 20	
			RT 55	
131. Deberá tomar acciones cuando el escaneo de archivos falle o exista sobre carga en el motor de antivirus.	X		ET 20	
			RT 56	
132. Detección dispositivos infectados con bots, analizando el tráfico de la red utilizando una tecnología multicapa.	X		ET 20	
			RT 51	
133. Detección y bloqueo de malware desconocido, ataques dirigidos y ataques de día cero.	X		ET 20	
			RT 56	
134. Detección y bloqueo de virus conocidos (Pre-infección) y transferencias de archivos.	X		ET 20	
			RT 56	
135. Detección y bloqueo de infección post-bot, prevención y la visibilidad de la amenaza.	X		ET 20	
			RT 57	
136. Debe hacer inspección sobre tráfico encriptado PPTP, L2TP, IPSec, SSL.	X		ET 20	



			RT 27- 42	
137. Debe soportar la configuración de políticas granulares basadas en IPs o usuarios.	X		ET 20	
			RT 47- 49	
12. Emulación y Mitigación de Amenazas				
138. 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.	X		ET 21	
139. 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.	X		ET 21	
			RT 56	
140. Protección contra ataques de día cero: La solución debe proteger contra amenazas de día cero, antes de que la firma estática sea creada.	X		ET 21	
			RT 56	
141. Debe prevenir archivos maliciosos antes de que lleguen a la red interna.	X		ET 21	
			RT 57	
142. Debe proteger de ataques dirigidos a sistemas operativos Windows en múltiples versiones.	X		ET 21	
			RT 54	



INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

143. La solución debe emular archivos mayores de 10mb.	X		ET 21	
			RT 58	
144. 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.	X		ET 21	
			RT 58	
145. Debe soportar al menos los siguientes protocolos: HTTP, HTTPS, SMTP, CIFS, FTP.	X		ET 21	
			RT 58	
146. Debe soportar descifrado de archivos transferidos en una comunicación cifrada SSL o TSL dentro de la misma caja.	X		ET 22	
			RT 58	
147. Debe soportar políticas granulares basadas en usuario.	X		ET 22	
			RT 48	
148. La solución debe ser capaz de reconstruir los archivos con los elementos que son seguros (imágenes, textos, tablas, entre otros).	X		ET 22	
			RT 59	
149. La solución debe eliminar las amenazas y eliminar contenido explotable, incluyendo el contenido activo y objetos incrustados	X		ET 22	
			RT 59	
150. 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.	X		ET 22	

23



			RT 59	
151. La solución debe mantener la flexibilidad con opciones de mantener el formato de archivo original y especificar el tipo de contenido que será eliminado.	X		ET 22 RT 60	
152. Se debe monitorear e inspeccionar la actividad y comportamiento que provoca el archivo inspeccionado en múltiples sistemas operativos y versiones de office.	X		ET 22 RT 61	
153. Se debe poder generar reportes detallados de la emulación, mitigación y eliminación de la amenaza.	X		ET 23 RT 61	
13. IPSec VPN				
154. 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).	X		ET 23	
155. La solución debe tener la posibilidad de soportar tanto un CA Interno provisto por un tercero.	X		ET 23 RT 62	
156. Debe poder validar la conexión VPN por medio de certificados digitales o llaves secretas.	X		ET 23 RT 62	



157. Debe ser soportado 3DES y AES-256 para las fases I y II de IKE.	X		ET 23	
			RT 63	
158. 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).	X		ET 23	
			RT 64	
159. Debe soportar integridad de datos con md5 y sha1.	X		ET 23	
			RT 63	
160. 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).	X		ET 23	
			RT 65	
161. Verificación de usuarios con autenticación de dos (2) factores.	X		ET 24	
			RT 66	
162. Debe incluir una función para la verificación de cumplimiento de requerimientos de seguridad mínimos de portátiles y Pcs.	X		ET 24	
			RT 67	
163. 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.	X		ET 24	
			RT 68	
164. Soporte para acceso remoto a aplicaciones corporativas para dispositivos smartphones, tablets o PCs.	X		ET 24	



			RT 68	
165. El administrador debe poder aplicar reglas de control de tráfico, al interior de la VPN.	X		ET 24	
			RT 69	

14. Inicio de Sesión y Monitoreo

166. Capacidad de integración con consola actual de Check Point con la que cuenta el Instituto. El IHSS posee actualmente una licencia de Management para cinco (5) Gateway, instalados en una versión de Check Point R80.40, la solución a adquirir se debe integrar a esta plataforma ya existente.	X		ET 24	La integración es transparente gracias a las licencias que poseen los equipos
167. Los equipos por adquirir deben ser capaces de hacer el envío de "logs" a la consola centralizada de Management Check Point.	X		ET 24	Esta configuración se aplicará una vez se instalen y configuren los equipos
168. Los equipos deben de lograr ser monitoreados desde la consola de management en elementos como CPU, licenciamiento y estado del hardware.	X		ET 24- 25	El licenciamiento de los 5 Gateway permitirá el monitoreo desde una consola centralizada

15. Soporte Técnico Local

169. Soporte técnico local (24x7x365), por el periodo de doce (12) meses; para el caso de averías, incidencias, configuraciones y/o consultas técnicas, incluyendo el soporte presencial o remoto, de acuerdo con lo descrito en el presente documento, bajo los siguientes niveles de criticidad:	X		ET 25	<p>Subsanar SEFISA: El Instituto requiere soporte 24x7x365, se solicita indicar si cumplen con este requerimiento.</p> <p>Respuesta SEFISA: En fecha 18 de noviembre de 2021, remite oficio donde confirma que el soporte técnico local ofertado es en un horario 24x7x365. 26</p>
--	---	--	----------	--

Nivel de Soporte	Tipo de Asistencia	Tiempo Máximo de Respuesta
Crítico	Presencial	2 horas
Moderado	Presencial/Asistencia Remota	6 horas
Bajo	Asistencia Remota/correc electrónico/teléfono	12 horas



170. El soporte técnico local será el encargado de aplicar las configuraciones y actualización (base de datos de firmas de ataques, firmas de malware, aplicaciones, categorías y filtrado URL) permanente de la solución.	X		ET 25	
171. El soporte técnico local será el encargado de la solución de incidentes y la apertura y seguimiento de casos con el fabricante cuando estos se requieran.	X		ET 25	
172. Se deberá entregar una hoja de escalamiento de incidentes el cual incluya números telefónicos, correos electrónicos y horarios de servicio, del equipo técnico que apoyará ante cualquier incidente.	X		ET 25	Subsanar SEFISA: Presentar hoja de escalamiento, conforme a lo solicitado. Respuesta SEFISA: En fecha 18 de noviembre de 2021, remite oficio donde adjunta hoja de escalamiento de incidentes.
173. Acceso Avanzado en un horario (8x7x365), a ingenieros especializados del Centro de Soporte Check Point.	X		ET 25	
174. Acceso en cualquier momento a la base de conocimientos en línea de Check Point con sus recursos y herramientas.	X		ET 26	
175. Cambio de hardware que incluyen el reemplazo de componentes y equipo defectuoso en caso de ser necesario; por dispositivos nuevos de iguales o mejores características.	X		ET 26	
176. Se requiere un mínimo de tres (3) visitas programadas para el mantenimiento preventivo de software y afinamiento de la solución durante la vigencia del contrato, donde se deben realizar la revisión de la configuración y operación del equipo de seguridad Check Point.	X		ET 26	
16. Tiempo de Entrega de los Equipos y Servicios				

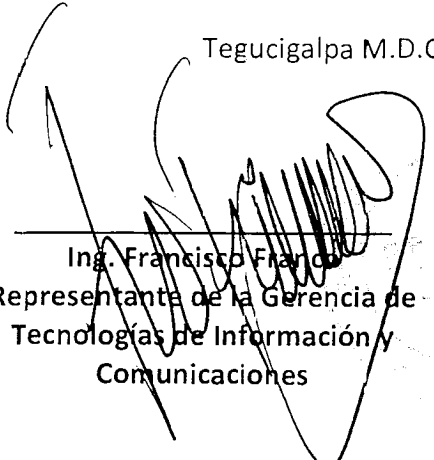


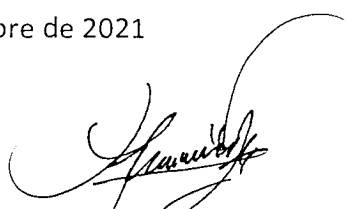
INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

177. El tiempo de entrega de los bienes, será en un plazo mínimo de cuarenta y cinco (45) días y un plazo máximo de sesenta (60) días calendario, después de recibir la orden de compras.	X		ET 26	
178. El Tiempo para la configuración, puesta en marcha y prueba de los bienes y servicios adquiridos, será de treinta (30) días calendario después de la recepción de los bienes.	X		ET 26	
17. Instalación y Verificación de la Solución				
179. La solución deberá ser aprovisionada, instalada, configurada, ajustada, verificada y puesta en marcha por el oferente; todos los componentes, accesorios, software y hardware necesarios para su instalación e implementación deberán ser provistos por el oferente.	X		ET 26	

SEGUNDO: Por lo tanto, se CONCLUYE que: la Empresa SISTEMAS EFICIENTES S.A. DE C.V. (SEFISA), cumple con las especificaciones técnicas solicitadas en las bases de licitación, mismas que están descritas en el cuadro de revisión de esta acta. Se solicito aclaración y subsanación para varios ítems, y la empresa dio respuesta en tiempo y forma. **TERCERO:** No habiendo más que consignar en este acto, se cierra en el mismo lugar el día treinta de noviembre del año dos mil veintiuno (3:00 p.m.) con la firma de los presentes.

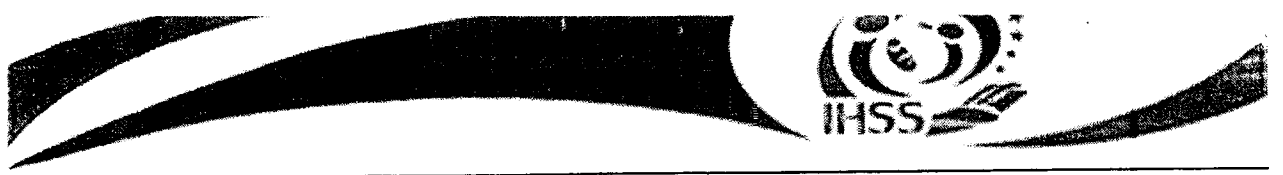
Tegucigalpa M.D.C. 30 de noviembre de 2021


Ing. Francisco Franco
Representante de la Gerencia de
Tecnologías de Información y
Comunicaciones


Ing. Jorge Arturo Echenique
Representante de la Gerencia de
Tecnologías de Información y
Comunicaciones

Gerencia de Tecnología de Información y Comunicación

8 piso, Edificio Administrativo, Tegucigalpa
Teléfono: (504) 2237-4840, consultas@ihss.hn
www.ihss.hn



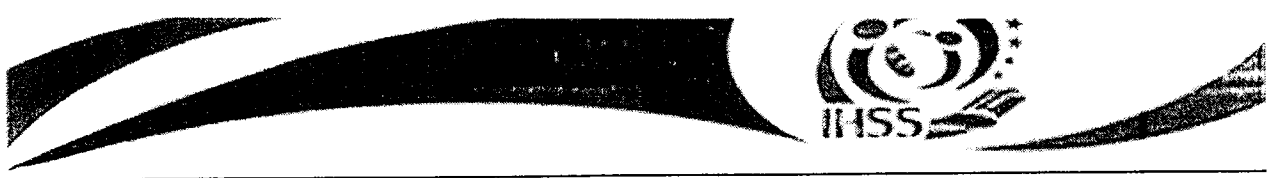
ACTA N° 2

EVALUACIÓN DE LA DOCUMENTACION LEGAL, LICITACION PRIVADA N° LP-017-2021 "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL IHSS".

En la ciudad de Tegucigalpa, Municipio del Distrito Central, a los diez días (10) días del mes de noviembre del año dos mil veintiuno (2021) siendo las nueve de la mañana (9:00 a.m.), reunidos en las oficinas de la Subgerencia de Suministros Materiales y Compras, del Instituto Hondureño de Seguridad Social, ubicado en el sexto piso del Edificio Administrativo, Barrio Abajo, Tegucigalpa M.D.C. los miembros de la Comisión de Evaluación de la LICITACION PRIVADA N° LP-017-2021 "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL IHSS", integrada de la siguiente manera: Abogada Belkis Erazo, Representante de la Unidad de Asesoría Legal, Ingeniero David Andino, Representante de la Subgerencia de Suministros Materiales y Compras, Licda. Yohana Vanessa Reconco, Representante de la Gerencia Administrativa y Financiera, con el objeto de revisar, analizar y evaluar la Documentación Legal, de las ofertas de conformidad a la SECCION I - INSTRUCCIONES A LOS OFERENTES, IO-09 DOCUMENTOS A PRESENTAR de las Bases de Licitación, para lo cual se procedió de la siguiente manera: **PRIMERO:** Se informa que mediante Resolución CI IHSS-GAYF N° 1630/04-10-2021 de fecha 04 de octubre del año 2021, se aprobaron las bases de la LICITACION PRIVADA N° LP-017-2021 "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL IHSS". **SEGUNDO:** Se informa que para este proceso de Licitación Privada N° LP-017-2021 se invitaron a las siguientes empresas: 1.- Sistemas Eficientes (SEFISA), Oficio No 960-DEI-IHSS-2021. 2.- Componentes El Orbe, Oficio No 961-DEI-IHSS-2021. **TERCERO:** Que la recepción y apertura de sobres que contienen las ofertas se realizó el día viernes 29 de octubre de 2021; por la comisión nombrada para tal efecto según consta en el memorando N° 3312-DEI-IHSS de fecha 27 de agosto de 2021, memorando N° 3972 de fecha 19 de octubre de 2021, memorando No 4080-DEI-IHSS de fecha 27 de octubre de 2021 y Acta No 1 de Recepción y Apertura de Ofertas. **CUARTO:** Se procedió a revisar la documentación de la oferta económica presentada por la única empresa participante: Sistemas Eficientes S.A. de C.V. (SEFISA), presenta una oferta económica, por un monto de Un millón, Setecientos Cuarenta y Cinco Mil Lempiras Exactos (L.1,745,000.00) presentando una garantía bancaria de mantenimiento de oferta No. 2413221, extendida por Banco Ficohsa, por un monto de Treinta y Cuatro Mil Lempiras Exactos (L.34,900.00), con una vigencia del 29 de octubre de 2021 hasta el 26 de febrero del año 2022. **QUINTO:** Se hace énfasis que la Disponibilidad Presupuestaria para la "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL IHSS" es por el valor de Seis Millones Cuatrocientos Cincuenta y Cuatro Mil Cuatrocientos Cincuenta y Dos Lempiras Exactos (L 6,454,452.00), la estructura presupuestaria que se detalla a continuación:

Fondo	ACCE Actividades Centrales
Área Funcional	AC 190004 Actividades Centrales
Centro Gestor	AC 217000 Gerencia de Tecnología Información y Comunicación
Pospre	39300 Útiles y Materiales Eléctricos
Pospre	42120 Equipos varios de oficina
Pospre	42600 Equipos para Computación
Pospre	47110 Construcciones y Mejoras de Bienes
Monto Disponible	L 6,454,452

Según consta en el memorando No 883-SGP/I-IHSS-2021 de fecha 16 de abril de 2021, firmado por el Licenciado José Lorenzo Coto, Subgerente de Presupuesto. **SEXTO:** Seguidamente los integrantes de la Comisión Evaluadora de esta licitación, en común acuerdo establecen que los miembros Abogada Belkis Erazo, Representante de la Unidad de Asesoría Legal, Ingeniero David Andino, Representante de la Subgerencia de Suministros Materiales y Compras, Licda. Yohana Vanessa Reconco, Representante de la Gerencia Administrativa y Financiera, procedan a revisar, analizar y evaluar la Documentación Legal, de las ofertas de conformidad a la SECCION I - INSTRUCCIONES A LOS OFERENTES, IO-09 DOCUMENTOS A PRESENTAR de las Bases de Licitación, de dicho análisis se concluye lo siguiente: Sistemas Eficientes S.A. de C.V. (SEFISA), debía de subsanar documentos legales y financieros solicitados en las bases de licitación, por lo que mediante Oficio No 001-CE-LP 017-2021 de fecha 05 de noviembre de 2021, se le solicitó que subsanara lo siguiente: 1) Fotocopia legible autenticada del RTN del Representante Legal de la empresa. Se le solicita debido a que no la presentó en su oferta. 2) Constancias de Institución Bancaria original o copia debidamente autenticada 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. Se le solicita debido a que la presentada en su oferta es copia y la misma no está autenticada. Finalizado el plazo establecido de cinco (5) días hábiles para la subsanación de la documentación legal y en cumplimiento al Artículo 132 del Reglamento de la Ley de Contratación de Estado, la Comisión de Evaluación procedió a verificar lo siguiente: La empresa Sistemas Eficientes S.A. de C.V. (SEFISA), subsanó toda la documentación solicitada. Por consiguiente la oferta presentada por esta empresa, pasa a la evaluación técnica. **SEPTIMO:** No habiendo más que consignar en este acto, se cierra en el mismo lugar y fecha arriba indicado siendo las once de la mañana (11:00 a.m.) con la firma de los presentes.

Abog. Belkis Erazo
Rep. Unidad de Asesoría Legal

Ing. David Andino.
Rep. Subgerencia de Suministros Materiales y Compras

Licda. Yohana Vanessa Reconco
Rep. Gerencia Administrativa y Financiera

ACTA N° 1

RECEPCION Y APERTURA DE OFERTAS DEL PROCESO DE LICITACION PRIVADA N° LP-017-2021 "ADQUISICIÓN E INSTALACIÓN DE UNA PLATAFORMA DE ALTA DISPONIBILIDAD CLUSTER CHECK POINT (2 NODOS) PARA EL INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL".

En la Ciudad de Tegucigalpa, Municipio del Distrito Central, a los veintinueve (29) días del mes de octubre del año dos mil veintiuno (2021), siendo las ocho de la mañana (8:00 a.m.), reunidos en el Lobby ubicado en el primer piso del Edificio Administrativo, Barrio Abajo, Tegucigalpa, M.D.C., los miembros nombrados, mediante memorando N° 4080-DEI-IHSS de fecha 27 de octubre de 2021 para la Recepción y Apertura del Proceso de **Licitación Privada N° LP-017-2021 "Adquisición e Instalación de Una Plataforma de Alta Disponibilidad Cluster Check Point (2 Nodos) para los Empleados del Instituto Hondureño de Seguridad Social, IHSS"** integrada de la siguiente manera: Abog. Belkys Erazo, representante de la Unidad de Asesoría Legal, Licda. Reina Victoria Durón, representante de la Subgerencia de Suministros Materiales y Compras, P.M. Ingrid Posadas, representante de la Gerencia Administrativa y Financiera, bajo el objetivo de Recepción y Apertura de las ofertas del proceso arriba descrito, se procede de la siguiente manera:

CLAUSULA PRIMERA: Mediante Resolución CI IHSS-GAYF N° 1630/04-10-2021 de fecha 4 de octubre de 2021, La Comisión Interventora aprobó las bases del proceso de Licitación Privada **N° LP-017-2021 "Adquisición e Instalación de Una Plataforma de Alta Disponibilidad Cluster Check Point (2 Nodos) para el Instituto Hondureño de Seguridad Social, IHSS"**. **SEGUNDA:** Para este proceso de Licitación Privada, se invitaron a las siguientes empresas: **1.- Sistemas Eficientes (SEFISA), 2.- Componentes El Orbe.TERCERA:** Siendo las diez de la mañana (10:00 a.m.) se cierra el Acto de recepción de ofertas. **CUARTA** Siendo las diez de la mañana con quince minutos (10:15 a.m.) se da inició a la apertura de sobres, se describen las empresas que presentaron ofertas para dicho proceso, **OFERENTE UNICO: Sistemas Eficientes (SEFISA)**, presenta una oferta económica, por un monto de **Un millón, Setecientos Cuarenta y Cinco Mil Lempiras Exactos (L.1,745,000.00)** presentando una garantía bancaria de mantenimiento de oferta No. 2413221, extendida por Banco Ficohsa, por un monto de **Treinta y Cuatro Mil Lempiras Exactos (L.34,900.00)**, con una vigencia del 29 de octubre de 2021 hasta el 26 de febrero del año 2022, dicha oferta consta de 47 folios útiles, conteniendo documentación Económica y Financiera, 60 folios útiles, conteniendo documentación legal y

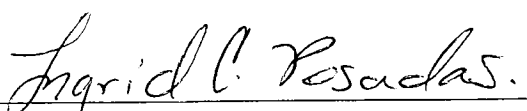
de Ofertas la en el mismo lugar el viernes 29 de octubre de 2021, siendo las diez de la mañana con cuarenta minutos (10:40 a.m.) y para constancia firmamos los abajo descritos



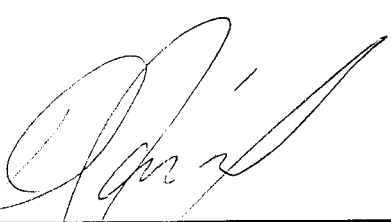
ABOG. BELKYS ERAZO
Rep. De La Unidad de Asesoría Legal



LICDA. REINA VICTORIA DURON
Rep. De La Subgerencia de Suministros,
Materiales y Compras



P.M. INGRID POSADAS
Rep. De La Gerencia Administrativa
Y Financiera



DANIEL LOPEZ
Representante de SEFISA



INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

MEMORANDO

No. 1800-GTIC-IHSS-2021

PARA: LIC. EDWIN MEDINA
Gerente Administrativo y Financiero

DE: ING. FRANCISCO FRANCO
Gerencia de Tecnologías de Información y Comunicaciones

ASUNTO: Autorización para la Adquisición e Instalación de una Plataforma de Alta Disponibilidad Clúster Check Point (2 nodos) para el IHSS.

FECHA: Lunes, 16 de agosto de 2021

Cordialmente solicito a Usted la autorización y gestiones administrativas necesarias para Adquisición e Instalación de una Plataforma de Alta Disponibilidad Clúster Check Point (2 nodos) para el IHSS, se recomienda que este proceso se realice mediante una Licitación Privada, este proceso es parte del PACC 2021.

Según certificación de canales enviada por el Fabricante Check Point Software Technologies Inc. (ver adjuntos), las únicas empresas autorizadas por el fabricante para vender el portafolio de soluciones y servicios Check Point, son las siguientes (sin ningún orden en particular):

SISTEMAS EFICIENTES (SEFISA)

Bulevar Morazán, Centro Morazán, Torre 2, piso 16, local 11613, Tegucigalpa Honduras
Teléfono: (504) 2236-9669 / 3297-2528

lmejia@sefisa.com

dlopez@sefisa.com

COMPONENTES EL ORBE

Colonia Lomas del Guijarro, Avenida, República Dominicana Torre Alfa 6to piso, 500 mts arriba del Ministerio Publico., Tegucigalpa 11101

Teléfono: (504) 2263-6274 / 8826-0912

tpaz@orbe.com.hn

eespinal@orbe.com.hn

Gerencia de Tecnología de Información y Comunicación

8 piso, Edificio Administrativo, Tegucigalpa

Teléfono: (504) 2263-4621, consultas@ihss.hn

www.ihss.hn

27
17 AGO 2021
Francisco Franco
B. S. S. P.
5

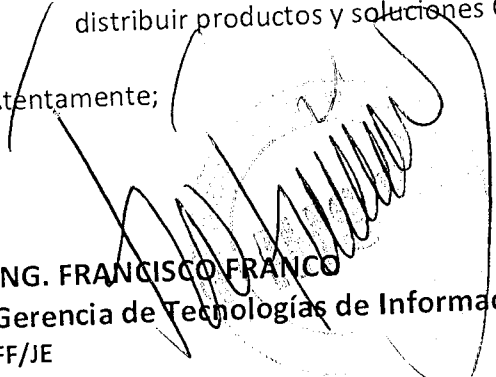


INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

Se adjuntan a este Memorando la siguiente documentación:

1. Justificación Técnicas para la Adquisición e Instalación de una Plataforma de Alta Disponibilidad Clúster Check Point (2 nodos) para el Instituto Hondureño de Seguridad Social (IHSS).
2. Especificaciones Técnicas para la Adquisición e Instalación de una Plataforma de Alta Disponibilidad Clúster Check Point (2 nodos) para el Instituto Hondureño de Seguridad Social (IHSS).
3. Memorando No 883-SGP/IHSS-2020, enviado por la Subgerencia de Presupuesto brindando la disponibilidad presupuestaria ítem No. 4, por un monto total de L.2,500,000.00.
4. Oferta técnica/económica de referencia, enviada por la empresa Sistemas Eficientes (SEFISA).
5. Carta enviada por Check Point Software Technologies Inc., informando la existencia de dos (2) socios calificados que pueden participar en el proceso de Adquisición e Instalación de una Plataforma de Alta Disponibilidad Clúster Check Point (2 nodos) para el IHSS.
6. Constancias de la Secretaria de Desarrollo Económico, donde certifica que SISTEMAS EFICIENTES (SEFISA) Y COMPONENTES EL ORBE, están autorizados para distribuir productos y soluciones Check Point.

Atentamente;


ING. FRANCISCO FRANCO

Gerencia de Tecnologías de Información y Comunicaciones

FF/JE

cc. archivo

Gerencia de Tecnología de Información y Comunicación
8 piso, Edificio Administrativo, Tegucigalpa
Teléfono: (504) 2263-4621, consultas@ihss.hn
www.ihss.hn



INSTITUTO HONDUREÑO DE SEGURIDAD SOCIAL

**MEMORANDO No.
10472-GAYF-2021**

PARA: **Ing. Francisco Franco**
Gerente de Tecnología de Información y Comunicación

DE: **Lic. Edwin Orlando Medina**
Gerente Administrativo y Financiero

ASUNTO: **Autorización Inicio de proceso**

FECHA: 17 de agosto de 2021

En referencia al Memorando 1800-GTIC-IHSS-2021 y de acuerdo al procedimiento administrativo, presupuestario y legal establecido y de acuerdo a las Disposiciones Generales del Presupuesto Vigente, se autoriza el inicio del proceso de adquisición de Instalación de Plataforma de Alta Disponibilidad Clúster Check Point (2 nodos) para el IHSS, por un monto de L.6,454,452.00. ✓

Asimismo se autoriza la inclusión en el PACC-2021, sino está incluido.

Se devuelve la información original.

Atentamente,

C: SGSMYC
Archivo

/Xiomara
17/08/2021 16:45

Gerencia Administrativa y Financiera, 9no. Piso Edificio Administrativo del IHSS
Teléfonos: (504) 2237-5183, 2237-4787 y 2237-3325 Ext. 1913-1914



INSTITUTO HONDUREÑO DE SEGURO SOCIAL

MEMORANDO No. 883-SGP/IHSS - 2021

Para: Ing. Francisco Franco
Gerente de Tecnologías de Información y Comunicaciones

De: Lic. José Lorenzo Coto
Subgerente de Presupuesto

Asunto: **DISPONIBILIDAD PRESUPUESTARIA**

Fecha: 16 de abril del 2021.



En respuesta a Memorando No. 955-GTIC-IHSS-2021 de fecha 15 de abril del 2021, para la adquisición de UPS, puerta antifuego, sensores para centros de datos, firewall y aire acondicionado de precisión redundancia, el cual esta contemplado en el PACC 2021, conforme al siguiente detalle:

No.	Descripcion	Inversion	Objeto del Gasto
1	Adquisicion de UPS- Centro de datos Hospitales (HE y HRN)	1,730,505.00	42600
2	Puerta Antifuego Centro de Datos Principal, BA	96,704.00	47110
3	Sensores de Humedad y Temperatura para el Centro de Datos principal, BA	127,243.00	39300
4	Firewall perimetral, centro de datos principal, BA	2,500,000.00	42600
5	Aire acondicionado de precision redundante, Centro de datos Principal, BA	2,000,000.00	42120
Total		L. 6,454,452.00	

Al respecto le informo que existe disponibilidad en la estructura presupuestaria que se detalla a continuación:

Fondo:	ACCE Actividades Centrales
Area Funcional:	AC190004 Actividades Centrales
Centro gestor:	AC217000 Gerencia de Tecnologia Informacion y Comunicacion
Pospre:	39300 Utiles y Materiales Electricos
Pospre:	42120 Equipos Varios de Oficina
Pospre:	42600 Equipo para Computacion
Pospre:	47110 Construcciones y Mejoras de Bienes
Monto disponible:	L 6,454,452.00

Atentamente,

C: Archivo
JLC-SYAR

Sub Gerencia de Presupuesto, Quinto piso, Edificio Administrativo, Tegucigalpa
Teléfono: (504) ext. 1306-1411, consultas@ihss.hn
www.ihss.hn

16 ABR 2021
Jorge E
3.15.2021