“RENOVACIÓN LICENCIAMIENTO DE SOFTWARE ANTIVIRUS PARA EL PODER JUDICIAL”

BASES DE LICITACIÓN PÚBLICA NACIONAL

N° 14-2022

RENOVACIÓN LICENCIAMIENTO DE SOFTWARE ANTIVIRUS PARA EL PODER JUDICIAL.

Fuente de Financiamiento:

FONDOS NACIONALES PROPIOS DEL PODER JUDICIAL

Honduras/Tegucigalpa 29/09/2022

Contenido

SECCION I – INSTRUCCIONES A LOS OFERENTES

IO-01 CONTRATANTE

El **Poder Judicial** tiene por objeto adquirir la "Renovación del Licenciamiento del Software de Antivirus ESET- EndPoint Protection Advanced, ESET- Mail Security for Exchange EndPoint Solutions G7 EDTD, SandBoxing en la Nube –ESET Dynamic Threat Defense del Poder Judicial, el cual brinda la protección para las computadoras de los usuarios, servidores, servicio de correo electrónico que conforman la plataforma tecnológica de este Poder del Estado." La Contratación de la Renovación del Licenciamiento será mediante proceso de Licitación Pública.

Según el periodo siguiente:
El proveedor que resulte adjudicado debe contar con disponibilidad inmediata para la recepción del bien objeto de la presente licitación.

La recepción del licenciamiento deberá ser inmediata, después de la adjudicación, el licenciamiento es en línea y la empresa adjudicada deberá asegurarse del registro de las mismas en los servidores del fabricante a nombre del **Poder Judicial de Honduras**.

El suministro de "LICENCIAS (RENOVACIÓN ESET ENDPOINT PROTECCION ADVANCED, ESET MAIL SECURITY FOR EXCHANGE ENDPOINT SOLUTIONS G7 EDTD, SANDBOXING EN LA NUBE –ESET DYNAMIC THREAT DEFENSE,)", con disponibilidad de entrega inmediata.

IO-02 TIPO DE CONTRATO

Como resultado de esta licitación se podrá otorgar un contrato de suministro, entre el ***Poder Judicial*** y el licitante ganador.

IO-03 OBJETO DE CONTRATACIÓN

El Poder Judicial necesita efectuar la renovación y continuidad de las 5,000 licencias del software antivirus ESET ENDPOINT PROTECCION ADVANCED, ESET MAIL SECURITY FOR EXCHANGE ENDPOINT SOLUTIONS G7 EDTD, SANDBOXING EN LA NUBE –ESET DYNAMIC THREAT DEFENSE. Con la finalidad de garantizar una adecuada protección de los equipos y sistemas informáticos que conforman la red tecnológica del Poder Judicial, siendo los objetivos específicos siguientes:

1. Renovar el licenciamiento se contará con la actualización, parches y soporte del fabricante que contienen las mejoras y correcciones de problemas de vulnerabilidad.
2. Renovar el licenciamiento permitirá la detección de virus y software maliciosos informáticos por medio de su base de datos actualizada.

3. Identificar de manera oportuna las vulnerabilidades existentes en los equipos de los usuarios y servidores.

IO-04 IDIOMA DE LAS OFERTAS

Las ofertas deberán presentarse en idioma español, incluso información complementaria como catálogos técnicos, etc. En caso de que la información complementaria esté escrita en idioma diferente al español, deberá acompañarse con la debida traducción de la Secretaría de Estado en los Despachos de Relaciones Exteriores y Cooperación.

IO-05 PRESENTACIÓN DE OFERTAS

Los oferentes presentarán su oferta, en original y copia parte legal, parte técnica y económica; **las páginas de la oferta deberán venir foliado, incluyendo las bases y cualquier otra información que se presente junto con la oferta**, rubricada tanto en el original como la copia. - Deberán venir en un solo sobre cerrado (no engrapado) y con sello de la empresa al reverso del mismo.

Rotulación de sobre: El sobre sellado que contendrá los documentos de oferta, un original y una copia, será rotulado de la siguiente manera: Parte Central:
COMISIÓN DE EVALUACION DE LA
LICITACIÓN PÚBLICA NACIONAL N° 14-2022
UNIDAD DE LICITACIONES
DIRECCIÓN ADMINISTRATIVA
TEGUCIGALPA, M.D.C.
HONDURAS, C.A.
Esq. Sup. Izquierda: Representante Legal y su Dirección Completa.
Esq. Inf. Izquierda: Oferta Licitación Pública Nacional N°. 14-2022
Esq. Sup. Derecha: Fecha de Recepción y apertura y Hora de apertura.
Dirección de Correo Electrónico de la empresa:

Orden en la presentación de las ofertas: Los documentos de la oferta, en original y copia, deberán estar organizados bajo las siguientes reglas de presentación y orden:

- Todas las ofertas se deberán presentar debidamente encuadernadas o empastadas.
- La Portada deberá contener el Nombre de la empresa que provea el Suministro, el Número de la Licitación y la Fecha de Apertura y Dirección de Correo Electrónico de la empresa.
- La oferta original contendrá
  1. Carta Propuesta: (Ver Anexo)
  2. Declaración Jurada (Ver Anexo)
  3. Garantía de Mantenimiento de Oferta: de acuerdo a lo establecido en estas bases.
  4. Documentos Legales de acuerdo al orden expuesto en estas bases.
  5. Documentos Técnicos.

El formato de la oferta deberá contener toda la información solicitada. La omisión de uno o varios de los renglones mencionados podrá dar lugar a descalificación de la propuesta a criterio de la

comisión de evaluación del Poder Judicial, dependiendo de la importancia relativa de la información remitida. La propuesta deberá ceñirse a las especificaciones.

Cada sección de la oferta debe ir con un separador indicando el nombre de la sección, de preferencia con colores que permitan su fácil manejo y debidamente foliada desde su inicio hasta la última página de la oferta.

La apertura de las ofertas se llevará a cabo con la recepción de un mínimo de una (1) oferta.

Una vez recibidos los sobres de las ofertas para la presente licitación, el Jefe de la Unidad de Licitaciones o delegado procederá a la apertura de las mismas, con la asistencia únicamente de las personas que comparezcan el día y la hora señalados en el aviso de publicación. Las ofertas serán recepcionadas, abiertas y leídas en el lugar indicado en la invitación a licitar, dándole lectura a lo siguiente: Nombre de la empresa, representante legal de la empresa, propuesta económica, garantía de mantenimiento de oferta equivalente al dos por ciento (2%) del monto total de la oferta, si la empresa presenta documentación en original y copia, numero de folios. De todo lo anterior se levantará el acta correspondiente, la cual será firmada por todos los asistentes al acto.

Ningún licitante podrá modificar su oferta después de que ésta haya sido abierta. El Poder Judicial se reserva el derecho de aceptar o solicitar aclaraciones que no alteren su contenido después de la apertura de ofertas.

El día ultimo de presentación de ofertas será: ***la fecha que indique la invitación a licitar***

La hora límite de presentación de ofertas será: ***la hora que indique la invitación a licitar***

Una copia del acta de apertura de ofertas será publicada en el sistema HonduCompras.

Los oferentes o sus representantes que deseen estar presente al momento de apertura de las ofertas deberán presentarse a la dirección siguiente*: Poder Judicial, atrás del Palacio de Justicia, edificio principal en el Salón de Sesiones de la Dirección Administrativa en el edificio que alberga las Oficinas del Nuevo Edificio Administrativo y de la Unidad de Licitaciones, colonia Miraflores Sur, Tegucigalpa, Honduras.*

IO-05.1 CONSORCIO

Cada Oferente presentará una sola Oferta, ya sea individualmente o como miembro de un Consorcio. 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.

IO-06 VIGENCIA DE LAS OFERTAS

Las ofertas deberán tener una vigencia mínima de CIENTO CUARENTA DIAS (140), calendarios contados a partir de la fecha de presentación de la oferta.

No obstante, en casos calificados y cuando fuere estrictamente necesario, el órgano contratante podrá solicitar la ampliación del plazo a todos los proponentes, siempre que fuere antes de la fecha prevista para su vencimiento. Si se ampliare el plazo de vigencia de la oferta, deberá también ampliarse el plazo de garantía de mantenimiento de oferta.

IO-07 GARANTIA DE MANTENIMIENTO DE OFERTA

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

Se aceptarán solamente fianzas y garantías bancarias emitidas por instituciones debidamente autorizadas y cheques certificados.

La garantía deberá tener una vigencia mínima de treinta (30) días adicionales, posteriores a la fecha de vencimiento de la vigencia de las ofertas.

IO-08 PLAZO DE ADJUDICACIÓN

La Licitación se adjudicará al oferente que, ajustándose a los requisitos establecidos en los documentos de licitación, presente la oferta más conveniente a los intereses del Poder Judicial y cumpla con lo establecido en la Ley de Contratación del Estado, su reglamento y el pliego de condiciones.

La oferta solo se considerará definitivamente adjudicada, cuando se emita el correspondiente Acuerdo de Adjudicación por el Honorable Magistrado Presidente del Poder Judicial**,** el cual será notificado por escrito.

Al oferente cuya oferta sea seleccionada se le notificará el lugar y fecha para formalizar el Contrato correspondiente.

IO-09 DOCUMENTOS A PRESENTAR

Cada oferta deberá incluir los siguientes documentos:

IO-09.1 DOCUMENTACIÓN LEGAL

Las firmas de las declaraciones juradas de los demás documentos debidamente autenticadas en otro certificado deberán ser presentadas conforme a lo que ordena el (Artículo 40 del Reglamento del Código de Notariado) debiéndose presentar dos (2) auténticas diferentes, una para documentos que sean fotocopias y otra para aquellas declaraciones juradas en donde consten firmas que deben ser autenticadas por Notario.

- Fotocopia autenticada de la escritura de constitución de la Empresa y sus modificaciones, si las hubiere, debidamente inscrita en el Instituto de la Propiedad Inmueble y Mercantil. (DS)
- Fotocopia autenticada del Poder de Representación y sus modificaciones si las hubiere, debidamente inscrito en el Instituto de la Propiedad Inmueble y Mercantil. (DS)
- Fotocopia del Documento Nacional de Identificación (DNI) y RTN del Representante de la Empresa. (DS)
- Carta Propuesta (ver anexo) (DNS)
- Garantía de Mantenimiento con indicación de la cláusula obligatoria (ver anexo) (DNS)
- Garantía de Cumplimiento con indicación de la cláusula obligatoria, en el caso de resultar adjudicado. (DS) (ver anexo)
- Declaración Jurada debidamente autenticada por Notario Público, donde se consigne que la Empresa y su Representante Legal, no están comprendidos en ninguno de los casos a que se refieren a los Artículos No. 15, y 16 de la Ley de Contratación del Estado. (ver anexo) (DS)
- Declaración Jurada debidamente autenticada en la que se consigne que la sociedad y su Representante Legal, no están comprendidos en los Artículos 36, 37,38,39, 40 y 41 de la Ley Especial Contra el Lavado de Activos. (ver anexo) (DS).
- Declaración Jurada, debidamente autenticada, de la entidad Garante, conforme a los artículos 241 y 242 del Reglamento de la Ley de Contracción del Estado (ver anexo) (DS) así mismo esta declaración debe ser tanto para garantía de mantenimiento como para cumplimiento en este último caso, para la empresa que sea adjudicada y la cual deberá presentarse en original firmada por el representante legal bancario o compañía de seguros y esta firma debe de estar debidamente autenticada por notario.
- Declaración Jurada sobre Integridad (ver anexo) (DS)
- Permiso de operación vigente extendido por la Alcaldía Municipal de su localidad. (DS)
- Constancia de Solvencia vigente emitida por el Instituto Hondureño de Seguridad Social, (IHSS) DS.
- Certificación o Constancia vigente de solicitud de inscripción en la Oficina Normativa de Contratación y Adquisiciones del Estado. (ONCAE). (DS)
- Constancia de inscripción y solvencia vigente de la Cámara de Comercio e Industria de su localidad (DS)-
- Constancia de solvencia vigente extendida por el Servicio de la Administración de Rentas, (SAR). (DS)
- Constancia de solvencia extendida por la Procuraduría General de la República, a favor de la sociedad y su representante legal de no haber sido objeto de resolución firme de cualquier contrato celebrado con la administración, vigente a la fecha de apertura de las ofertas de la presente licitación. (DS)

- Constancia de inscripción y solvencia vigente extendida por el Colegio profesional correspondiente a favor de la empresa y autorizado para participar en proyectos para el Poder Judicial (DS).
- Recibo de pago del Documento Base, extendido por la Pagaduría Especial del Poder Judicial.

Los oferentes deberán presentar, junto con su propuesta, la declaración jurada a que hace referencia el Artículo 29 del Reglamento de la Ley de Contratación del Estado, y en caso de que el oferente resultare adjudicatario, y no adjuntó los siguientes documentos a su oferta al momento de la apertura, deberá presentar las correspondientes constancias acreditando, entre otros, lo siguiente: a) No haber sido objeto de sanción administrativa firme en dos (2) o más expedientes por infracciones tributarias durante los últimos cinco (5) años. b) No haber sido objeto de resolución firme de cualquier contrato celebrado con la Administración; c) Encontrarse al día en el pago de sus cotizaciones o contribuciones al Instituto Hondureño de Seguridad Social, de conformidad con lo previsto en el artículo 65 párrafo segundo, literal b) reformado de la Ley del Seguro Social. Dichas constancias deberán ser expedidas por la Dirección Ejecutiva de Ingresos, Procuraduría General de la República y el Instituto Hondureño de Seguridad Social u otras autoridades competentes. Asimismo, el pliego podrá disponer la obligación del Oferente, si fuere sociedad mercantil, de acreditar para los fines de los artículos 15 numeral 7) y 16 de la Ley, la composición de su capital, mediante certificación expedida por el órgano societario correspondiente. El órgano responsable de la contratación también requerirá información a la Oficina Normativa de Contratación y Adquisiciones acerca de la prohibición establecida en el numeral 5) del citado artículo 15 de la Ley." Las mismas podrán ser presentadas por el Oferente en caso que resultare adjudicado en un término de cinco (5) días hábiles contados a partir del día siguiente de su Notificación; cualquier defecto u omisión que no se contemple en el artículo antes citado y no sea subsanado en tiempo, se atendrá a lo dispuesto en el artículo 132 del Reglamento último párrafo y su oferta no será considerada.

Los anteriores documentos deben ser de la empresa mercantil, vigentes y en caso de presentar fotocopia de los mismos deben estar debidamente autenticados.

Todo oferente deberá cumplir en su totalidad con los requisitos legales indicados en el pliego de condiciones como no subsanable (NS), para ser evaluados posteriormente, técnica y económicamente. –

Documentos no subsanables

1. Formulario de Presentación de Oferta la cual debe presentarse de conformidad con el formato que se acompaña firmado y sellado por el Representante Legal
2. Lista de Precios, firmado y sellado por el Representante Legal de la Empresa.
3. Garantía de Mantenimiento de Oferta original.

NOTA:

1. Todos los documentos que no sean originales deberán ser autenticados (Una autentica de copias).
2. Los documentos firmados por el Representante Legal de la empresa que se anexe a la oferta deberán estar autenticados (Una autentica de firmas).

3. Autentica de la Declaración Jurada, debidamente autenticada, de la entidad Garante, conforme a los artículos 241 y 242 del Reglamento de la Ley de Contracción del Estado (ver anexo) (DS) así mismo esta declaración debe ser tanto para garantía de mantenimiento como para cumplimiento en este último caso, para la empresa que sea adjudicada y la cual deberá presentarse en original firmada por el representante legal bancario o compañía de seguros y esta firma debe de estar debidamente autenticada por notario.

Los siguientes se consideran defectos u omisiones subsanables siempre y cuando no impliquen modificaciones del precio, objeto y condiciones ofrecidas según Artículo 132 del Reglamento de la Ley de Contratación del Estado:

a) La falta de copia de la oferta
b) La falta de literatura descriptiva
c) La omisión de datos que no tengan relación directa con el precio
d) La inclusión de datos en unidades de medida diferentes
e) La falta de presentación de la credencial de inscripción en el registro de proveedores y contratistas
f) Y los demás permitidos por la Ley de Contratación del Estado y su Reglamento.

Se permitirá subsanar errores u omisiones dentro de los **cinco (5) días hábiles administrativos** después de recibida la notificación por el oferente, lo anterior en base al Artículo 5 párrafo 2 y 50 de la Ley de Contratación del Estado y 132 del Reglamento de la Ley de Contratación del Estado.

La comisión Evaluadora corregirá los errores meramente aritméticos que se hubieren detectado durante el examen de las ofertas, y se le hará del conocimiento del oferente. Artículo 133 párrafo segundo del Reglamento de la Ley de Contratación del Estado.

IO-09.2 INFORMACIÓN FINANCIERA

Documentos probatorios de acceso inmediato a dinero en efectivo por al menos ***SEISCIENTOS MIL LEMPIRAS (L. 600,000.00)***, pueden ser evidencias de montos depositados en caja y bancos, constancias de;

- Créditos abiertos otorgados por instituciones bancarias, nacionales o extranjeras, créditos comerciales, etc.
- Copia autenticada del Balance General del último ejercicio fiscal inmediato anterior sellado y timbrado por el contador general.
- Copia autenticada del Estado de Resultado del último ejercicio fiscal inmediato anterior sellado y timbrado por el contador general.
- Autorización para que el **Poder Judicial** pueda verificar la documentación presentada con los emisores.

IO-09.3 INFORMACIÓN TÉCNICA

A continuación, se presenta la descripción técnica del material objeto de adquisición:

No	TIPO DE LICENCIA	Especificaciones Técnicas Incluye	Descripción	CANTIDAD
1	ESET ENDPOINT PROTECTION ADVANCED	A) Protection para Endpoints-ESET Endpoint Security, Antivirus y Antispyware.	Protección Avanzada en múltiples niveles para PC, Smartphones y máquinas virtuales. Elimina todos los tipos de amenazas, incluyendo virus, rootkits, gusanos y spyware	5,000
		B) Sandboxing en la nube-ESET Dynamic Threat Defense	Protección Mejorada contra ransomware y amenazas 0-day a través del sandboxing en la nube	
		C) Protection para Correos Electrónicos - ESET Mail Security For Exchange Endpoint Solutions G7 Edtd	Bloquean spam y malware a nivel del servidor, antes de que lleguen a las casillas de correo de los usuarios.	

IO-09.4 INFORMACIÓN ECONÓMICA

- Formulario de la oferta, este formulario deberá ser llenado en letras y números con el precio total ofertado, solicitándose no alterar su forma.

- Formulario de Lista de Precios: Es el detalle individual de la partida cotizada en la oferta, debidamente firmado y sellado. La omisión de cualquier dato referente a precio unitario por partida, monto y número de la licitación, así como cualquier otro aspecto sustancial que impida o límite de manera significativa el análisis, comparación u evaluación de las ofertas, será motivo de descalificación de esta según sea el caso. Si "El Oferente" No presenta el formato "Lista de Precios" se entenderá que no presento la oferta.

- El valor total de la oferta deberá comprender todos los impuestos correspondientes y costos asociados hasta la entrega de los bienes ofertados al Poder Judicial en el lugar y fechas especificados en estas bases.

IO-09.5 DOCUMENTO QUE DEBEN PRESENTARSE ANTES DE LA FIRMA DEL CONTRATO (OFERENTE GANADOR)

SEGÚN EL ARTÍCULO 30 DEL REGLAMENTO DE LA LEY DE CONTRATACIÓN DEL ESTADO

1. Constancia de no haber sido objeto de sanción administrativa firme en dos (2)

o más expedientes por infracciones tributarias durante los últimos cinco (5) años, emitida por la SAR;

2. Constancia de no haber sido objeto de resolución firme de cualquier contrato celebrado con la Administración, emitida por la PGR;
3. Constancia de Encontrarse al día en el pago de sus cotizaciones o contribuciones al Instituto Hondureño de Seguridad Social, de conformidad con lo previsto en el artículo 65 párrafo segundo, literal b) reformado de la Ley del Seguro Social.
4. Certificación de Inscripción en el Registro de proveedores y contratistas del Estado, emitida por la ONCAE

Las mismas podrán ser presentadas por el Oferente en caso que resultare adjudicado en un término de cinco (5) días hábiles contados a partir del día siguiente de su Notificación; cualquier defecto u omisión que no se contemple en el artículo antes citado y no sea subsanado en tiempo, se atendrá a lo dispuesto en el artículo 132 del Reglamento último párrafo y su oferta no será considerada.

IO-10 ACLARACIONES DE LOS DOCUMENTOS DE LICITACIÓN

Todo aquel que haya obtenido de manera oficial los documentos de licitación y que requiera alguna aclaración sobre los mismos deberá comunicarse con **El ente contratante**, mediante correo electrónico **[bvasquez@poderjudicial.gob.hn]** o en su defecto por escrito a la dirección y contacto siguiente [***Unidad de Licitaciones del Poder Judicial***]. **El ente contratante** responderá por escrito todas las solicitudes de aclaración, enviando copia a todos los que hayan obtenido los pliegos de condiciones, describiendo y resolviendo sus interrogantes planteadas.

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).

Para efectos de recibir aclaraciones las mismas será admitida antes de los [***ocho (08) días calendarios antes de la fecha de apertura de oferta***], toda aclaración recibida después de la fecha límite no se tomará en cuenta.

IO-10. I ENMIENDAS A LOS DOCUMENTOS DE LICITACIÓN

El **Poder Judicial** podrá en cualquier momento antes del vencimiento del plazo para la presentación de ofertas, enmendar los documentos mediante la emisión de una Adenda.

Toda enmienda emitida formara parte integral de los documentos y deberá ser comunicada por escrito ya sea en físico o correo electrónico a todos los que hayan obtenido los pliegos de condiciones.

Las enmiendas se publicarán además en el Sistema de Información de Contratación y Adquisiciones del Estado de Honduras HONDUCOMPRAS (www.honducompras.gob.hn).

El [Poder Judicial] podrá prorrogar el plazo de presentación de ofertas a fin de dar a los posibles oferentes un plazo razonable para que pueda tomar en cuenta las enmiendas en la preparación de sus ofertas de conformidad a los cambios indicados en las mismas.

IO-11 EVALUACIÓN DE OFERTAS

Las ofertas serán evaluadas de acuerdo a la siguiente rutina de fases acumulativas[1]:

FASE I VERIFICACIÓN LEGAL

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

ASPECTO VERIFICABLE	CUMPLE	NO CUMPLE
La Garantía de Mantenimiento de Oferta asegura los intereses del **Poder Judicial** (la especie de garantía es aceptable y la vigencia y el valor son suficientes) (DNS).		
Carta Propuesta (DNS).		
La sociedad ofertante se encuentra legalmente constituida		
Quien firma la oferta tiene la atribución legal para hacerlo		
Copia Autenticada del Documento Nacional de identificación(DNI) del Representante Legal		
Copia autenticada de RTN del oferente y Representante Legal.		
Declaración Jurada sobre las Prohibiciones o Inhabilidadesprevistas en los artículos 15 y 16 de la Ley de Contratación del Estado (Autenticada)		
Constancia de inscripción en el Registro de Proveedores y Contratistas del Estado, extendida por la ONCAE.[2]		

[1] Para efecto de evaluación, sino pasa la fase legal, ya sea un documento sustancial, según lo indicado en el Pliego de Condiciones no se deberá seguir evaluando ni pasar a la siguiente fase de evaluación.

[2] En el caso en que el oferente presente la constancia de estar inscrito en el Registro de Proveedores, no deberá presentar copia autenticada de escritura de constitución y sus reformas debidamente inscritas y notificadas, poder del representante legal del oferente, constancia de colegiación del oferente y copia autenticada de RTN del oferente, a menos que alguno de los datos haya cambiado y no haya sido reportado a la ONCAE.

La Declaración Jurada de la empresa y de su representante legal de no estar comprendido en ninguno de los casos señalados de los artículos 36,37,38,39,40 y 41 de la Ley Especial Contra el Lavado de Activos Fotocopia del Permiso de Operación de la Municipalidad correspondiente, vigente.		
Otros Documentos agregados por la institución		
Declaración debidamente autenticada emitida por la institución garante que extendió la garantía de mantenimiento, conforme lo dispuesto en el artículo 241 y 242 del reglamento de la ley de contratación del estado. Se aclara que esta misma declaración deberá ser extendida en caso de adjudicación, por la institución garante que extienda la garantía de cumplimiento.		
Declaración jurada sobre integridad		
Constancia de Solvencia vigente emitida por el Instituto Hondureño de Seguridad Social (IHSS).		
Constancia de inscripción y solvencia de la Cámara de Comercio e Industria de su localidad.		
Constancia de solvencia vigente extendida por el (Servicio de la Administración de Rentas (SAR).		
Constancia de solvencia extendida por la Procuraduría General de la República, a favor de la empresa y su representante legal de no tener juicios pendientes con el Estado.		
Garantía de Cumplimiento con indicación de la cláusula obligatoria, en caso de que resultare adjudicada su oferta.		

FASE II, EVALUACIÓN FINANCIERA

ASPECTO VERIFICABLE	CUMPLE	NO CUMPLE
Demuestra acceso inmediato a dinero en efectivo por al menos ***[SEISCIENTOS MIL LEMPIRAS (L. 600,000.00)]***		

Copia autenticada del Balance General del último ejercicio fiscal inmediato anterior sellado y timbrado por el contador general.		
Copia autenticada del Estado de Resultado del último ejercicio fiscal inmediato anterior sellado y timbrado por el contador general		
Autoriza que el **Poder Judicial** pueda verificar la documentación presentada.		

FASE III, EVALUACIÓN TÉCNICA

A continuación, se presenta la descripción técnica del material objeto de adquisición:

Evaluación de la Documentación Técnica

Aspecto evaluable en documentos técnicos		Cumple	No Cumple
Documentación	El oferente proporcionará documentación técnica o folletos en los cuales se muestre la marca, la calidad y la descripción de especificaciones técnicas del software.		
	La presentación de folletos o descripción técnica, para verificar el cumplimiento de cada una de las especificaciones técnicas.		
	Certificación emitida por la autoridad competente mediante la cual se constate que el oferente es representante o distribuidor de las marcas ofertadas o en su caso Autorización vigente del Fabricante del Software al oferente como distribuidor.		

Evaluación de Condiciones y Servicios

Condiciones y servicios		Cumple	No Cumple	No. Pág. referencia documentación técnica
Garantía	Se debe incluir una cobertura y soporte directo con el fabricante por 2 años.			

Condiciones y servicios		Cumple	No Cumple	No. Pág. referencia documentación técnica
	Las atenciones de situaciones críticas deben ser atendidas por el fabricante y el envío de partes en caso de emergencia, el fabricante debe enviarlo directamente hacia las oficinas del cliente sin ningún costo adicional.			
	El soporte de debe ser 24*7*365 con tiempo de respuesta al siguiente día laborable una vez reportado el caso con el fabricante.			
Soporte Técnico	El Oferente de la solución debe proporcionar documentación que evidencie sus procesos para atención de casos y solución de incidentes técnicos.			
Cumplimiento del Oferente	El oferente debe acreditar experiencia en proyectos similares desarrollados en el país >= 5 años (especificar).			
	El oferente deberá comprobar el nivel de "Partner" o distribución que mantiene con el fabricante, a fin de garantizar el servicio técnico y asesoría post implementación que puede ofrecer.			
	El oferente deberá presentar carta emitida por el fabricante, firmada por el representante legal, donde reconocen al oferente como un canal autorizado para la venta y soporte de sus productos.			

ALCANCE

El alcance de la renovación del licenciamiento del software antivirus es aplicable para todos los equipos informáticos conectados a la red tecnológica y distribuidos a nivel nacional en cada sede judicial. Incluye computadoras de usuarios, servidores, y las diferentes plataformas tecnológicas virtuales del Poder Judicial.

Especificaciones Técnicas

Cliente ESET ENDPOINT Security

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
Sistemas Operativos Compatibles	Incorpore garantía de compatibilidad extendida para sistemas operativos 32bits y 64bits:		
	- Microsoft Windows® 11,10,8.1, 8, 7 SP1 y/o superior		
	- Microsoft Windows Server 2019,2016,2012R2,2012,2008R2, 2008 y/o superior		
	- Microsoft Windows Server Core 2019, 2016, 2012R2, 2012, 2008R2, 2008 Core y/o superior		
	- OS X 10.6 y/o superior		
	- RedHat, Debian, Ubuntu, Suse, Fedora & Mandriva así como la mayoría de distribuciones basadas en gestor de paquetes RPM y DEB		
	Incorpore garantía de compatibilidad extendida para las siguientes versiones de servidores de correo electrónico:		
	- Microsoft Exchange Server 2019, 2016, 2013, 2010, 2007 y/o superior		
	Licenciamiento otorgado deberá poseer garantía y cobertura sobre los sistemas operativos indicados como requeridos, se acepta un solo y único lote de licenciamiento que involucre a todos los sistemas indicados; puntualmente deberá ocuparse una única clave de activación, llave o similar para todos los productos contratados e indicados como compatiblemente requeridos.		
	Licenciamiento adquirido en su totalidad deberá poder ser administrado por una única consola de administración, todos los productos adquiridos para los sistemas operativos indicados como compatibles deberán poderse administrar integralmente desde una única consola validada e implementada en la red interna corporativa.		

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
Aspectos Generales	Incorpore protección en tiempo real contra todo tipo de malware; incluyendo virus, gusanos, troyanos, spyware, phishing, rootkit, adware, riskware, keyloggers y/o otros códigos maliciosos nuevos y desconocidos. Específicamente para dicho fin no deberá depender de que el Sistema Operativo del "ENDPOINT/Cliente" tenga las actualizaciones y Service Pack al día		
	Incorpore protección contra virus boot, virus macros, virus residentes en RAM, virus de acción directa, virus encriptados, virus polimórficos, virus de FAT, etc.		
	Deberá integrar sandbox incorporado en el propio producto, con el objetivo de contener amenazas, emularlas, detectarlas y eliminarlas; dicha protección en particular deberá ser capaz de observar el comportamiento en tiempo real de cualquier binario en memoria operativa (RAM), siendo capaz de detectar basado en patrones de comportamiento & ML amenazas nuevas y desconocidas del tipo 0Day, APT's y/o cualquier tipo de código malicioso emergente.		
	Incorpore motor heurístico proactivo y preciso de tecnología avanzada, dicho motor debe ser propio y no de terceros fabricantes y/o colaboraciones externas ajenas a casa matriz.		
	Incorpore detección de virus en archivos compactados, sin importar el número de niveles de compresión, en los formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y/o otros.		
	Integralmente hablando producto instalado en el computador no deberá presentar fragmentación para su correcto funcionamiento (múltiples módulos instalados en el computador reflejados en programas instalados "Agregar/Quitar Programas" no serán aceptados, exceptuando únicamente al agente de conexión).		
	Deberá permitir importar o exportar configuraciones de clientes de manera fácil, vía archivos xml livianos y transportables.		

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
	Incorpore capacidad de poder enviar a los centros de soporte técnico las muestras de virus o códigos maliciosos, con la finalidad de que puedan ser analizados, y clasificados para su contingencia inmediata directamente desde la interfaz gráfica.		
	Incorpore capacidad de generar casos de soporte vía la interfaz gráfica de la solución.		
	Incorpore chequeo y control de Actualizaciones para Microsoft Windows, dicho control debe ser capaz de ser configurado para reportar diferentes niveles de actualización o desactivar el informe de las mismas.		
	Toda configuración a nivel de clientes, deberá poder ser posible realizarse desde consola administrativa y funcionalmente podrá gestionarse integralmente desde una única consola administrativa centralizada. Queda implícitamente descrito todos los productos adquiridos deberán administrarse desde una sola consola de administración, no importando el sistema operativo sobre el cual hayan sido implementados.		
	Incorpore compatibilidad nativa en su interfaz gráfica con dispositivos que integren tecnología TouchScreen.		
	Incorpore cache local de inspección a fin de mejorar el rendimiento en equipos virtualizados, explícitamente la cache de inspección local deberá validar si los ficheros fueron inspeccionados previamente por otro equipo en la red y en todo caso no forzar inspección local si el mismo es sano e inocuo al sistema a fin de acelerar el proceso de inspección. Dicha cache en aceleración de inspección antivirus/antimalware deberá de ser compatible con cualquier plataforma de virtualización, así como funcionalmente hablando no deberá requerir la instalación de ningún plugin o complemento instalado y evidente desde "Control Panel -> Agregar o Quitar programas".		

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
	Solución a contratarse deberá provisionar capacidad para generar CD y/o USB Booteables, los cuales posean capacidad de análisis para la inspección de malware en máquinas que no cuenten con la protección de solución contratada o requieran del uso de los mismos con el fin de eliminar cualquier código malicioso, así mismo dichos medios deben poder ser actualizados vía Internet inmediatamente después del arranque desde los mismos.		
	Solución a contratarse deberá provisionar capacidad para generar CD y/o USB Booteables, los cuales deberán ofrecer como medio alternativo las siguientes herramientas de diagnóstico y asistencia técnica remota con proveedor o fabricante:		
	• Gparted		
	• MemTest86+		
	• Teamviewer		
	• Otras aplicaciones para recibir asistencia remota		
	• Otras		
	Solución a contratarse deberá cumplir con estándares AMTSO, identificables y validables en cada una de sus pruebas de evidencia técnica; de igual forma fabricante antivirus deberá figurar en el listado de miembros activos de AMTSO.		
	Solución a contratarse deberá incluir múltiples capas de seguridad, que deberán operar en forma conjunta y en su defecto tener capacidad de proteger independientemente si alguna de ellas no detecta en un momento dado el vector de ataque; dicho de otra forma, deberá garantizar proteger al ENDPOINT final con diferentes métodos de protección y múltiples capas de seguridad comprobables según documentación de fabricante.		
	Incorpore protección a nivel Kernel, previniendo la desactivación y/o alteración por un tercero y/o código malicioso.		

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
	Incorpore auto-protección del núcleo y componentes de la suite de seguridad a nivel ASLR & DEP, así como funcionalmente no requiera de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”.		
	Incorpore protección en tiempo real contra cualquier alteración al estado del kernel antivirus, imposibilitando detenerlo o dejarlo inoperativo para protección del computador donde ha sido implementado.		
	Integre protección nativa de aprendizaje automático, la cual deberá incluir mecanismos de simulación/detección mediante redes neurales y al menos seis algoritmos de clasificación integrados, dicho módulo de protección deberá coadyuvar en la detección de cualquier tipo de código malicioso nuevo y/o desconocido; así como funcionalmente no debe requerir de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”.		
	Deberá integrar protección nativa a nivel UEFI que permita comprobar y aplicar seguridad para el entorno previo al inicio y arranque del equipo, dicho modulo deberá detectar componentes maliciosos en el firmware (UEFI/BIOS); funcionalmente no debe requerir de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”.		
	Incorpore capacidad de protección por contraseña de acceso al propio motor antivirus, a fin de que no pueda ser alterada configuración de la propia solución y/o alteración al estado de protección del computador.		
	Instalación de producto podrá realizarse tanto localmente como remotamente desde su consola administrativa; en el término local se entiende se requiere pre compilación de un paquete todo-en-uno para la instalación del producto el cual contenga las pre configuraciones y niveles de seguridad básicos aplicables a la estación de trabajo, así mismo incorpore en un solo paso la unión y sincronización a consola administrativa.		

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
	Comunicación entre clientes administrados (ENDPOINTS) y servidor de administración deberá realizarse mediante conexión SSL cifrada; dicha conexión deberá ser evidente y descrita en el log de estado del agente de conexión mediante cualquier navegador web para fines de validación o auditoria.		
	Agente de conexión deberá provisionar log transaccional de referencia, así como en forma simultánea deberá mostrar su estado de conexión y descripción general de sincronizaciones a servidor administrativo; dicho log deberá ser accesible desde cualquier navegador web y en forma dinámica deberá variar en forma automática a fin de evidenciar cualquier problema de comunicación o falla de transferencia y/o comunicación cifrada en la línea del tiempo		
	Agente de conexión deberá reportar en forma precisa todo software de terceros y/o fabricante contratado ubicado en el computador que figure como instalado en el equipo donde ha sido instalado.		
	Agente de conexión deberá reportar en forma precisa todo hardware instalado en el computador donde ha sido instalado, reportando con precisión todo lo referente al hardware presente.		
	Agente de conexión deberá soportar instalación de software de terceros, no delimitando e incluyendo cualquier aplicativo (EXE) que desee ejecutarse o instalarse en los computadores administrados.		
	Solución a contratarse requiere soporte técnico directo del fabricante y que este pueda prestarlo localmente en formato 24x7x365; el mismo en sus modalidades deberá garantizarse ya sea en forma presencial, remota, chat en línea, correo electrónico y/o vía telefónica mediante número local; en caso que la empresa adjudicada por alguna razón no pueda proporcionarlo.		
	Nativamente consola de administración deberá poseer soporte para equipos y/o servidores clonados sean estos físicos o virtuales, de forma tal que el identificador por disco o volumen de disco no constituya un problema para identificar individualmente cada equipo administrado.		

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
	Deben incluirse medias de Instalación originales provistas por el fabricante, evidenciables mediante certificado de originalidad provisto por el fabricante y entregado con las mismas.		
	Ofertante deberá demostrar experiencia comprobable con respecto al software ofertado para implementación, administración y soporte técnico dentro del territorio nacional que rige este evento para al menos cinco años calendario; en resguardo a los bienes de la institución, así como garantía de cumplimiento del ofertante, no se aceptaran ofertas que no proporcionen la información solicitada y/o bien no presenten las pruebas que así lo demuestren.		
	Ofertante deberá demostrar poseer experiencia comprobable para la implementación, administración y soporte técnico en al menos dos clientes que sean igual o superiores a la cantidad total de nodos computacionales que rige este evento; dicho requerimiento será admitido como válido en formalidad únicamente para referencias dentro de territorio nacional, no se aceptaran referencias del extranjero o que no coincidan en su totalidad con el producto ofertado, en resguardo a los bienes de la institución, así como garantía de cumplimiento del ofertante, no se aceptaran ofertas que no proporcionen la información solicitada y/o bien no presenten las pruebas que así lo demuestren		
	Ofertante deberá garantizar en totalidad de forma y por escrito que todo tipo de soporte técnico solicitado por esta institución ya sea con el propio ofertante y/o con el fabricante en cualesquiera de sus modalidades 24x7x365 sea totalmente gratuito, así como garantice en su totalidad no aplique ninguna restricción por horas de servicio o similar.		
	Ofertante deberá demostrar mediante documento oficial de fabricante, el mismo es un proveedor autorizado para el territorio nacional de sus productos; en caso fabricante no posea oficinas locales dentro del territorio nacional deberá indicarse como no cumplimiento al requerimiento específico sobre dicho aspecto, así como deberá considerarse todo documento que ampare al ofertante como proveedor oficial de solución ofertada cumpla con protocolo de ley para la nacionalización de documentos procedentes del extranjero.		

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
Host-based Intrusion Prevention System	Incorpore tecnología de control HIPS para estaciones de trabajo y servidores sobre plataforma Microsoft Windows, así como funcionalmente no requiera de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”.		
	Incorpore HIPS con capacidades avanzadas de protección y funcionalmente sea capaz de realizar las siguientes acciones básicas, pero no limitadas requeridas:		
	• Bloquear archivos y/o aplicaciones para ejecución		
	• Permitir ejecutar archivos y/o aplicaciones basados en rutas de acceso y/o ficheros en particular		
	• Bloquear archivos y/o carpetas contra escritura y/o acceso		
	• Permitir escritura y/o acceso para archivos y/o carpetas		
	• Bloquear escritura y/o modificación a llaves del registro de sistema		
	Incorpore tecnología avanzada que permita prevenir la explotación de vulnerabilidades en las aplicaciones más comunes; principalmente pero no limitado control de explotación para navegadores web, PDF, clientes de correo electrónico, aplicaciones MS Office & Java.		
	Incorpore motor de inspección avanzada en memoria operativa que brinde protección contra el malware moderno que ocupa técnicas de cifrado y/o ofuscación.		
	Incorpore protección avanzada contra la deshabilitación y/o modificación del propio motor de protección antivirus por parte de terceros y/o algún código malicioso, dicha función deberá reflejarse en el componente HIPS cargado en el sistema.		
	Deberá incorporar protección especializada contra ataques del tipo ransomware, la misma deberá ser explícitamente visible dentro del apartado de configuración del producto final adquirido; específicamente el módulo especializado para la prevención del ransomware deberá detectar y bloquear procesos cuyo comportamiento encuadre con la conducta del ransomware en general.		

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
Actualizaciones	Las actualizaciones rutinarias de la base de definición de firmas, deberán de ser pequeñas e incrementales; tanto para actualizaciones rutinarias como para repositorios de distribución (mirror). Se consideran como pequeñas e incrementales a las actualizaciones rutinarias menores a 1MB por cada firma de definición.		
	Funcionalmente una actualización rutinaria, debe ser capaz de actualizar firmas antivirus, módulos y/o componentes del sistema antivirus; no incluyendo, pero no limitando la versión de familia del producto contratado y/o futuras versiones del producto adjudicado.		
	Incorpore capacidad para que un cliente instalado (endpoint) pueda convertirse en repositorio de actualizaciones (mirror), con el fin de poder actualizar otros clientes desde este o poder extraer los archivos de actualización y trasladarlos manualmente a otros clientes "stand-alone"; funcionalmente no debe requerir la instalación de módulos adicionales para tales fines, así como no deberá reflejarse como componente adicional en "Agregar/Quitar Programas"		
	Deberá poseer factibilidad para actualizar de forma manual todos sus componentes y definiciones de virus, en computadoras sin ningún tipo de conectividad a red; es decir, en status "stand-alone".		
	Las actualizaciones de distribución de firmas rutinarias (repositorios de firmas) deberán proveerse a los clientes antivirus internos, mediante servicio HTTP/HTTPS incluido en el propio motor del producto instalado así mismo deberá poder ofrecerse métodos de autenticación básica o vía NTLM a fin de proteger contra el acceso de terceros a firmas antivirus de distribución local; dicha opción deberá integrarse mas no quedar limitada y/o restringida como medio para distribución de firmas mediante motores FTP/Shares de terceros; funcionalmente no debe requerir la instalación de módulos adicionales para tales fines así como no deberá reflejarse como componente adicional en "Agregar/Quitar Programas".		

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
	Las actualizaciones diarias y rutinarias de los componentes del producto se deberán realizar en tiempo real desde Internet o vía LAN Server (Mirror), en forma automática y sin necesidad de intervención del usuario.		
	Producto deberá poder actualizar automáticamente desde una unidad extraíble que contenga los ficheros rutinarios de actualización sin intervención alguna del usuario local o bien del personal técnico.		
Filtrado de Red y/o Protocolos de Comunicación	Incorpore capacidad de filtrado de protocolos, para todo el tráfico de red; teniendo opción de analizar todo tipo de comunicación saliente/entrante. Funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		
	Incorpore escaneo y limpieza de paquetes en tráfico HTTP, FTP, SMTP y POP3; tanto en los servidores como en las computadoras personales.		
	Incorpore filtrado e inspección de protocolos seguros (HTTPS, SMPTS, POP3S, FTPS, entre otros), funcionalmente hablando debe ser capaz de filtrar cualquier comunicación de red segura así como no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".		
	Incorpore capacidad de excluir aplicaciones, direcciones IP y/o rangos de direcciones del filtrado de protocolos e inspección al tráfico de red.		
	Incorpore capacidad de analizar todo el tráfico de red o bien indicar puertos y/o aplicaciones en particular a inspeccionar a nivel de filtrado de protocolos.		
	Incorpore filtrado básico para listas URL y/o IP de acceso; de tal forma que se pueda controlar efectivamente accesos a los listados estáticos definidos, ya sean sobre comunicación en texto plano (HTTP) o sobre protocolos seguros (HTTPS); funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
	Incorpore pluguin para el filtrado, análisis y detección antimalware en los clientes de correo electrónico Microsoft Outlook, Windows Mail & Windows Live Mail; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".		
	Incorpore tecnología avanzada que integre capas de seguridad previa al host a fin de prevenir la explotación de vulnerabilidades a nivel de red desde host remotos o locales, en forma explícita se requiere proteger el ENDPOINT final contra vulnerabilidades conocidas que puedan afectar a nivel de red aun así no exista parche local instalado en el equipo que desea protegerse Mail; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".		
Firewall & IDS	Incorpore firewall/cortafuegos avanzado de doble vía; capaz de filtrar bidireccionalmente el tráfico de red ya sea este entrante o saliente, funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		
	El firewall/cortafuegos incorporado deberá ser totalmente administrable desde cliente o desde consola administrativa, así como deberá poseer modo de solución rápida a problemas comunes guiados intuitivamente desde la propia interfaz del producto.		
	Firewall/Cortafuegos incorporado deberá poseer facilidad para la definición de redes de confianza mediante parámetros de detección que faculten identificar si en realidad dispositivo protegido se encuentra en una red "segura" o bien se requiere un modo superior de protección en una red nueva y desconocida.		
	Incorpore IDS (Intrusion Detection System) de host para la prevención de acceso no autorizado al computador a nivel de capa de red, funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
	Incorpore protección anti "BOTNETS", la cual faculte a la solución bloquear el acceso y comunicación a una red botnet así como alertar al usuario de dicha acción y anomalía detectada; funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		
	Incorpore Control de Vulnerabilidades a nivel de capa de red, el cual deberá inspeccionar y proteger a los protocolos más ampliamente utilizados SMB, RPC y RDP; evitando con dicho fin la propagación del malware, ataques de red dirigidos y la explotación de vulnerabilidades para las que un parche de seguridad aún no está disponible o ha sido desplegado, funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		
Antispam	Incorpore solución antispam a nivel endpoint y posea filtrado para protocolo SMTP, POP3 & IMAP en forma transparente e integrada al producto sin requerir instalación de módulos y/o agentes en el computador; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".		
	Incorpore plugin para el filtrado, análisis y clasificación antispam en los clientes de correo electrónico Microsoft Outlook, Windows Mail & Windows Live Mail; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".		
	Provea capacidad de generar listas blancas/negras para el filtrado del correo electrónico en la estación de trabajo final y en los clientes de correo electrónico indiciados como compatibles; dicha acción deberá de ser posible realizarse desde el propio producto y/o consola de administración, así como permitirá definir dominios y/o direcciones en cada uno de estos apartados.		
Web Filtering	Integre capacidad de Web Filtering basado en categorías, siendo posible definir políticas basadas en grupos de usuario y/o usuarios (tanto a nivel AD como también mediante autenticación local); no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".		

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
	Incorpore capacidad de Web Filtering mediante grupos de categorías, haciendo factible el agrupamiento de múltiples y diferentes categorías de inspección URL para una misma regla de navegación.		
	Faculte permitir y/o denegar el acceso URL estáticos mediante reglas configuradas en el Web Filtering.		
	Provea posibilidad de agrupamiento en políticas de filtrado URL, siendo factible sumar diferencialmente los accesos y/o denegaciones a fin de aplicar una política final de maquina o grupo de usuarios.		
	Integre capacidad para la generación de logs y sincronización de los mismos a consola corporativa, de acuerdo a cada una de las acciones tomadas en concordancia con la regla URL definida ya sea bloqueo o permisión según sea el caso; dicho log deberá contener toda la información detallada desde el URL bloqueado/permitido hasta el usuario/equipo detectado así como hora/fecha y descripción integra del evento; no debe requerir de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control".		
	Integre capacidad Web Filtering sobre sitios URL que ocupen protocolo seguro (HTTPS); no debe requerir de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control".		
	Toda regla y/o política para el control URL, deberá poder ser fijada por horarios, días de la semana en particular y/o por usuarios en específico.		
Device Control	Incorpore capacidades de "Device Control" administrables ya sea localmente o en forma remota desde su consola administrativa; no debe requerir de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"		
	Incorpore capacidades de "Device Control" avanzadas, con el fin de delimitar, denegar o permitir dispositivos portátiles y/o medios extraíbles tales como:		
	• Dispositivos de almacenamiento USB		
	• Dispositivos ópticos CD/DVD		

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
	• Impresoras USB		
	• Dispositivos de almacenamiento Firewire		
	• Dispositivos Bluetooth		
	• Tarjetas lectoras de memoria		
	• Dispositivos de imagen		
	• Modems		
	• Puertos LPT/COM		
	• Dispositivos portátiles (móviles)		
	Incorpore funciones avanzadas para el control de dispositivos siendo posible aplicar reglas con el fin de delimitar, denegar o permitir de acuerdo a las siguientes condiciones del dispositivo periférico conectado:		
	• Marca		
	• Modelo		
	• Serie		
	Incorpore funciones avanzadas para el control dispositivos siendo capaz de asignar políticas de acuerdo a grupos de trabajo local o grupos dinámicos mediante un Directorio Activo; así mismo provea extensión de operación por usuario local y/o usuarios de un Directorio Activo.		
	Incorpore funciones avanzadas para el control de dispositivos mediante grupos de "dispositivos", siendo posible asignar reglas y/o directrices mediante grupos pre-establecidos de dispositivos con el fin de facilitar administración, así como el control adecuado de los dispositivos conectados a las estaciones de trabajo		
	Toda regla y/o política para el control de dispositivos, deberá poder ser fijada por horarios, días de la semana en particular y/o por usuarios en especifico		
Endpoint Detection and Response	Incorpore capacidades extendidas para mitigar riesgos extendidos que puedan ser identificados con facilidad mediante una solución específica del tipo Endpoint Detección and Response		

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
	Deberá incorporar sofisticada de detección y respuesta que permita identificar comportamientos anómalos		
	Funcionalmente no deberá de depender de alguna consola ubicada en la nube o fuera de las instalaciones de la dependencia, toda funcionalidad requerida es del tipo local, así como deberá permitir en cualquier línea del tiempo inspeccionar, monitorizar o evaluar registros auditables recopilados por la herramienta de Detección y Respuesta solicitada		
	Funcionalmente deberá extender las capacidades de detección del endpoint local y al menos permitir detectar y/o responder ante:		
	• Detectar las amenazas persistentes avanzadas		
	• Detener los ataques sin archivos		
	• Bloquear las amenazas 0-day		
	• Protegerse del ransomware		
	• Neutralizar los ataques patrocinados por el estado		
	Funcionalmente deberá ser capaz de indicar con precisión cualquier script ejecutado mediante powershell, dicha funcionalidad deberá proporcionar evidencia total de la línea de comandos ejecutada (strings del script y/o código fuente del mismo)		
	Deberá proporcionar una detección única basada en el comportamiento y en la reputación de archivos, dicha reputación de ficheros deberá estar al día y en constante evaluación mediante telemetría global, misma que deberá permitir en tiempo real evaluar la reputación del fichero, proceso o script analizado		
	Deberá permitir configurar la sensibilidad de las reglas de detección para diferentes grupos de computadoras o usuarios, así como permitir eliminar fácilmente las falsas alarmas que pudiese causar alguna regla de detección manual incorporada por el equipo de seguridad de la información		
	Deberá permitir combinar criterios como nombre de archivo, ruta, hash, paths, línea de comandos y firmante de aplicación con la finalidad de con precisión las condiciones de activación de las alertas.		

PROTECCIÓN	ESPECIFICACIÓN TÉCNICA	CUMPLE	NO CUMPLE
	Deberá permitir ubicar con facilidad cualquier comportamiento sospechoso inclusive para eventos pasados, mismo que deberá representarse por cualquier regla de detección nueva agregada.		
	Deberá permitir al menos históricos de tres meses consecutivos, mismos que podrán ser evaluados dinámicamente ya sea mediante reglas de detección nuevas o reputación de ficheros obtenidos por indicadores de amenazas de terceros (IOC's) y telemetría global.		
	Deberá permitir ubicar cualquier indicador de compromiso de forma tal que permita determinar si una amenaza ya existía antes de la emisión de alerta para alguna regla estática configurada.		
	Deberá incluir reglas de detección integradas, así como deberá permitir crear propias reglas para responder a los incidentes detectados		
	Funcionalmente deberá permitir bloquear, detener o eliminar cualquier fichero o proceso mediante reglas de acción automatizadas o bien mediante intervención manual de algún operador de seguridad encargado internamente, dicha funcionalidad deberá ser extendida para ejecutar la misma acción sobre todos los computadores en forma simultánea.		
	Deberá permitir mayor visibilidad de lo ocurrido en cada computador respecto a ficheros, scripts y/o procesos en general		
	Deberá permitir importar o exportar todas sus reglas de detección o acción a formatos XML		
	• Deberá proporcionar visibilidad total de lo ocurrido, siendo capaz de identificar el origen de una afección en particular, misma visibilidad deberá ser total y no solo representada en una imagen estática, posibilitando de dicha manera descubrir la naturaleza del origen y causa de afección.		

ESET Mail Security For Exchange ENDPOINT Solutions G7 Edtd

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
Sistemas Operativos Compatibles	Incorpore garantía de compatibilidad extendida para sistemas operativos 32bits y 64bits:		
	• Microsoft Windows® 11,10, 8.1, 8, 7, Vista, XP SP3 y/o Superior		
	• Microsoft Windows Server 2019,2016,2012R2, 2012, 2008R2, 2008 y/o Superior		
	• Microsoft Windows Server Core 2019,2016,2012R2, 2012, 2008R2, 2008 Core y/o Superior		
	• OS X 10.6 y/o superior		
	• RedHat, Debian, Ubuntu, Suse, Fedora & Mandriva así como la mayoría de distribuciones basadas en gestor de paquetes RPM y DEB		
	Incorpore garantía de compatibilidad extendida para las siguientes versiones de servidores de correo electrónico: • Microsoft Exchange Server 2019, 2016, 2013, 2010, 2007		
	Licenciamiento otorgado deberá poseer garantía y cobertura sobre los sistemas operativos indicados como requeridos, se acepta un solo y único lote de licenciamiento que involucre a todos los sistemas indicados; puntualmente deberá ocuparse una única clave de activación, llave o similar para todos los productos contratados e indicados como compatiblemente requeridos		
	Licenciamiento adquirido en su totalidad deberá poder ser administrado por una única consola de administración, todos los productos adquiridos para los sistemas operativos indicados como compatibles deberán poderse administrar integralmente desde una única consola validada e		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	implementada en la red interna corporativa		
Aspectos Generales	Producto por adquirirse deberá ser totalmente gestionado, así como compatible con consola de administración interna ocupada para el efecto que por nombre se identifica como ESET Security Management Center, formalmente se deberá certificar compatibilidad desde sitio de fabricante donde se corrobore que el producto ofertado sea totalmente compatible con la consola de seguridad ocupada internamente.		
	Incorpore protección en tiempo real contra todo tipo de malware; incluyendo virus, gusanos, troyanos, spyware, phishing, rootkit, adware, riskware, keyloggers y/o otros códigos maliciosos nuevos y desconocidos. Específicamente para dicho fin no deberá depender de que el Sistema Operativo del "Endpoint/Cliente" tenga las actualizaciones y Service Pack al día		
	Incorpore protección contra virus boot, virus macros, virus residentes en RAM, virus de acción directa, virus encriptados, virus polimórficos, virus de FAT, etc		
	Deberá integrar sandbox incorporado en el propio producto, con el objetivo de contener amenazas, emularlas, detectarlas y eliminarlas; dicha protección en particular deberá ser capaz de observar el comportamiento en tiempo real de cualquier binario en memoria operativa (RAM), siendo capaz de detectar basado en patrones de comportamiento & ML amenazas nuevas y desconocidas del tipo 0Day, APT's y/o cualquier tipo de código malicioso emergente.		
	Incorpore motor heurístico proactivo y preciso de tecnología avanzada, dicho motor debe ser propio y no de terceros fabricantes y/o colaboraciones externas ajenas a casa matriz.		
	Incorpore detección de virus en archivos compactados, sin importar el número de niveles de compresión, en los formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y/u otros.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Integralmente hablando producto instalado en el computador no deberá presentar fragmentación para su correcto funcionamiento (múltiples módulos instalados en el computador reflejados en programas instalados "Agregar/Quitar Programas" no serán aceptados, exceptuando únicamente al agente de conexión).		
	Deberá permitir importar o exportar configuraciones de clientes de manera fácil, vía archivos xml livianos y transportables.		
	Incorpore capacidad de poder enviar a los centros de soporte técnico las muestras de virus o códigos maliciosos, con la finalidad de que puedan ser analizados, y clasificados para su contingencia inmediata directamente desde la interfaz gráfica.		
	Incorpore capacidad de generar casos de soporte vía la interfaz gráfica de la solución.		
	Incorpore chequeo y control de Actualizaciones para Microsoft Windows, dicho control debe ser capaz de ser configurado para reportar diferentes niveles de actualización o desactivar el informe de las mismas.		
	Toda configuración a nivel de clientes, deberá poder ser posible realizarse desde consola administrativa y funcionalmente podrá gestionarse integralmente desde una única consola administrativa centralizada. Queda implícitamente descrito todos los productos adquiridos deberán administrarse desde una sola consola de administración, no importando el sistema operativo sobre el cual hayan sido implementados.		
	Incorpore compatibilidad nativa en su interfaz gráfica con dispositivos que integren tecnología TouchScreen.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Incorpore cache local de inspección a fin de mejorar el rendimiento en equipos virtualizados, explícitamente la cache de inspección local deberá validar si los ficheros fueron inspeccionados previamente por otro equipo en la red y en todo caso no forzar inspección local si el mismo es sano e inocuo al sistema a fin de acelerar el proceso de inspección. Dicha cache en aceleración de inspección antivirus/antimalware deberá de ser compatible con cualquier plataforma de virtualización, así como funcionalmente hablando no deberá requerir la instalación de ningún plugin o complemento instalado y evidente desde "Control Panel -> Agregar o Quitar programas"		
	Solución a contratarse deberá provisionar capacidad para generar CD y/o USB Booteables, los cuales posean capacidad de análisis para la inspección de malware en máquinas que no cuenten con la protección de solución contratada o requieran del uso de los mismos con el fin de eliminar cualquier código malicioso, así mismo dichos medios deben poder ser actualizados vía Internet inmediatamente después del arranque desde los mismos.		
	Solución a contratarse deberá provisionar capacidad para generar CD y/o USB Booteables, los cuales deberán ofrecer como medio alternativo las siguientes herramientas de diagnóstico y asistencia técnica remota con proveedor o fabricante: - Gparted - MemTest86+ - Teamviewer - Otras aplicaciones para recibir asistencia remota - Otras		
	Solución a contratarse deberá cumplir con estándares AMTSO, identificables y validables en cada una de sus pruebas de evidencia técnica; de igual forma fabricante antivirus deberá figurar en el listado de miembros activos de AMTSO		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Solución a contratarse deberá incluir múltiples capas de seguridad, que deberán operar en forma conjunta y en su defecto tener capacidad de proteger independientemente si alguna de ellas no detecta en un momento dado el vector de ataque; dicho de otra forma, deberá garantizar proteger al ENDPOINT final con diferentes métodos de protección y múltiples capas de seguridad comprobables según documentación de fabricante.		
	Incorpore protección a nivel Kernel, previniendo la desactivación y/o alteración por un tercero y/o código malicioso.		
	Incorpore auto-protección del núcleo y componentes de la suite de seguridad a nivel ASLR & DEP, así como funcionalmente no requiera de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		
	Incorpore protección en tiempo real contra cualquier alteración al estado del kernel antivirus, imposibilitando detenerlo o dejarlo inoperativo para protección del computador donde ha sido implementado.		
	Integre protección nativa de aprendizaje automático, la cual deberá incluir mecanismos de simulación/detección mediante redes neurales y al menos seis algoritmos de clasificación integrados, dicho módulo de protección deberá coadyuvar en la detección de cualquier tipo de código malicioso nuevo y/o desconocido; así como funcionalmente no debe requerir de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Deberá integrar protección nativa a nivel UEFI que permita comprobar y aplicar seguridad para el entorno previo al inicio y arranque del equipo, dicho modulo deberá detectar componentes maliciosos en el firmware (UEFI/BIOS); funcionalmente no debe requerir de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		
	Incorpore capacidad de protección por contraseña de acceso al propio motor antivirus, a fin de que no pueda ser alterada configuración de la propia solución y/o alteración al estado de protección del computador.		
	Instalación de producto podrá realizarse tanto localmente como remotamente desde su consola administrativa; en el término local se entiende se requiere pre compilación de un paquete todo-en-uno para la instalación del producto el cual contenga las pre configuraciones y niveles de seguridad básicos aplicables a la estación de trabajo, así mismo incorpore en un solo paso la unión y sincronización a consola administrativa.		
	Comunicación entre clientes administrados (endpoints) y servidor de administración deberá realizarse mediante conexión SSL cifrada; dicha conexión deberá ser evidente y descrita en el log de estado del agente de conexión mediante cualquier navegador web para fines de validación o auditoria.		
	Agente de conexión deberá provisionar log transaccional de referencia, así como en forma simultánea deberá mostrar su estado de conexión y descripción general de sincronizaciones a servidor administrativo; dicho log deberá ser accesible desde cualquier navegador web y en forma dinámica deberá variar en forma automática a fin de evidenciar cualquier problema de comunicación o falla de transferencia y/o comunicación cifrada en la línea del tiempo.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Agente de conexión deberá reportar en forma precisa todo software de terceros y/o fabricante contratado ubicado en el computador que figure como instalado en el equipo donde ha sido instalado		
	Agente de conexión deberá reportar en forma precisa todo hardware instalado en el computador donde ha sido instalado, reportando con precisión todo lo referente al hardware presente.		
	Agente de conexión deberá soportar instalación de software de terceros, no delimitando e incluyendo cualquier aplicativo (EXE) que desee ejecutarse o instalarse en los computadores administrados.		
	Solución a contratarse requiere soporte técnico directo del fabricante y que este pueda prestarlo localmente en formato 24x7x365; el mismo en sus modalidades deberá garantizarse ya sea en forma presencial, remota, chat en línea, correo electrónico y/o vía telefónica mediante número local; en caso que la empresa adjudicada por alguna razón no pueda proporcionarlo.		
	Nativamente consola de administración deberá poseer soporte para equipos y/o servidores clonados sean estos físicos o virtuales, de forma tal que el identificador por disco o volumen de disco no constituya un problema para identificar individualmente cada equipo administrado.		
	Deben incluirse medias de Instalación originales provistas por el fabricante, evidenciables mediante certificado de originalidad provisto por el fabricante y entregado con las mismas.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Ofertante deberá demostrar experiencia comprobable con respecto al software ofertado para implementación, administración y soporte técnico dentro del territorio nacional que rige este evento para al menos cinco años calendario; en resguardo a los bienes de la institución, así como garantía de cumplimiento del ofertante, no se aceptaran ofertas que no proporcionen la información solicitada y/o bien no presenten las pruebas que así lo demuestren.		
	Ofertante deberá demostrar poseer experiencia comprobable para la implementación, administración y soporte técnico en al menos dos clientes que sean igual o superiores a la cantidad total de nodos computacionales que rige este evento; dicho requerimiento será admitido como válido en formalidad únicamente para referencias dentro de territorio nacional, no se aceptaran referencias del extranjero o que no coincidan en su totalidad con el producto ofertado, en resguardo a los bienes de la institución, así como garantía de cumplimiento del ofertante, no se aceptaran ofertas que no proporcionen la información solicitada y/o bien no presenten las pruebas que así lo demuestren.		
	Ofertante deberá garantizar en totalidad de forma y por escrito que todo tipo de soporte técnico solicitado por esta institución ya sea con el propio ofertante y/o con el fabricante en cualesquiera de sus modalidades 24x7x365 sea totalmente gratuito, así como garantice en su totalidad no aplique ninguna restricción por horas de servicio o similar		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Ofertante deberá demostrar mediante documento oficial de fabricante, el mismo es un proveedor autorizado para el territorio nacional de sus productos; en caso fabricante no posea oficinas locales dentro del territorio nacional deberá indicarse como no cumplimiento al requerimiento específico sobre dicho aspecto, así como deberá considerarse todo documento que ampare al ofertante como proveedor oficial de solución ofertada cumpla con protocolo de ley para la nacionalización de documentos procedentes del extranjero		
Host-based Intrusion Prevention System	Incorpore tecnología de control HIPS para estaciones de trabajo y servidores sobre plataforma Microsoft Windows, así como funcionalmente no requiera de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		
	Incorpore HIPS con capacidades avanzadas de protección y funcionalmente sea capaz de realizar las siguientes acciones básicas, pero no limitadas requeridas:		
	• Bloquear archivos y/o aplicaciones para ejecución		
	• Permitir ejecutar archivos y/o aplicaciones basados en rutas de acceso y/o ficheros en particular.		
	• Bloquear archivos y/o carpetas contra escritura y/o acceso.		
	• Permitir escritura y/o acceso para archivos y/o carpetas.		
	• Bloquear escritura y/o modificación a llaves del registro de sistema.		
	• Incorpore tecnología avanzada que permita prevenir la explotación de vulnerabilidades en las aplicaciones más comunes; principalmente pero no		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	limitado control de explotación para navegadores web, PDF, clientes de correo electrónico, aplicaciones MS Office & Java.		
	• Incorpore motor de inspección avanzada en memoria operativa que brinde protección contra el malware moderno que ocupa técnicas de cifrado y/o ofuscación.		
	• Incorpore protección avanzada contra la deshabilitación y/o modificación del propio motor de protección antivirus por parte de terceros y/o algún código malicioso, dicha función deberá reflejarse en el componente HIPS cargado en el sistema.		
	• Deberá incorporar protección especializada contra ataques del tipo ransomware, la misma deberá ser explícitamente visible dentro del apartado de configuración del producto final adquirido; específicamente el módulo especializado para la prevención del ransomware deberá detectar y bloquear procesos cuyo comportamiento encuadre con la conducta del ransomware en general.		
Actualizaciones	Las actualizaciones rutinarias de la base de definición de firmas, deberán de ser pequeñas e incrementales; tanto para actualizaciones rutinarias como para repositorios de distribución (mirror). Se consideran como pequeñas e incrementales a las actualizaciones rutinarias menores a 1MB por cada firma de definición.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Funcionalmente una actualización rutinaria, debe ser capaz de actualizar firmas antivirus, módulos y/o componentes del sistema antivirus; no incluyendo, pero no limitando la versión de familia del producto contratado y/o futuras versiones del producto adjudicado.		
	Incorpore capacidad para que un cliente instalado (endpoint) pueda convertirse en repositorio de actualizaciones (mirror), con el fin de poder actualizar otros clientes desde este o poder extraer los archivos de actualización y trasladarlos manualmente a otros clientes "stand-alone"; funcionalmente no debe requerir la instalación de módulos adicionales para tales fines así como no deberá reflejarse como componente adicional en "Agregar/Quitar Programas".		
	Deberá poseer factibilidad para actualizar de forma manual todos sus componentes y definiciones de virus, en computadoras sin ningún tipo de conectividad a red; es decir, en status "stand-alone".		
	Las actualizaciones de distribución de firmas rutinarias (repositorios de firmas) deberán proveerse a los clientes antivirus internos, mediante servicio HTTP/HTTPS incluido en el propio motor del producto instalado así mismo deberá poder ofrecerse métodos de autenticación básica o vía NTLM a fin de proteger contra el acceso de terceros a firmas antivirus de distribución local; dicha opción deberá integrarse mas no quedar limitada y/o restringida como medio para distribución de firmas mediante motores FTP/Shares de terceros; funcionalmente no debe requerir la instalación de módulos adicionales para tales fines así como no deberá reflejarse como componente adicional en "Agregar/Quitar Programas".		
	Las actualizaciones diarias y rutinarias de los componentes del producto se deberán realizar en tiempo real desde Internet o vía LAN Server (Mirror), en forma automática y sin necesidad de intervención del usuario.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Producto deberá poder actualizar automáticamente desde una unidad extraíble que contenga los ficheros rutinarios de actualización sin intervención alguna del usuario local o bien del personal técnico.		
Filtrado de Red y/o Protocolos de Comunicación	Incorpore capacidad de filtrado de protocolos, para todo el tráfico de red; teniendo opción de analizar todo tipo de comunicación saliente/entrante. Funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		
	Incorpore escaneo y limpieza de paquetes en tráfico HTTP, FTP, SMTP y POP3; tanto en los servidores como en las computadoras personales.		
	Incorpore filtrado e inspección de protocolos seguros (HTTPS, SMPTS, POP3S, FTPS, entre otros), funcionalmente hablando debe ser capaz de filtrar cualquier comunicación de red segura así como no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".		
	Incorpore capacidad de excluir aplicaciones, direcciones IP y/o rangos de direcciones del filtrado de protocolos e inspección al tráfico de red.		
	Incorpore capacidad de analizar todo el tráfico de red o bien indicar puertos y/o aplicaciones en particular a inspeccionar a nivel de filtrado de protocolos.		
	Incorpore filtrado básico para listas URL y/o IP de acceso; de tal forma que se pueda controlar efectivamente accesos a los listados estáticos definidos, ya sean sobre comunicación en texto plano (HTTP) o sobre protocolos seguros (HTTPS); funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Incorpore plugin para el filtrado, análisis y detección antimalware en los clientes de correo electrónico Microsoft Outlook, Windows Mail & Windows Live Mail; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".		
	Incorpore tecnología avanzada que integre capas de seguridad previa al host a fin de prevenir la explotación de vulnerabilidades a nivel de red desde host remotos o locales, en forma explícita se requiere proteger el endpoint final contra vulnerabilidades conocidas que puedan afectar a nivel de red aun así no exista parche local instalado en el equipo que desea protegerse Mail; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".		
Firewall & IDS	Incorpore firewall/cortafuegos avanzado de doble vía; capaz de filtrar bidireccionalmente el tráfico de red ya sea este entrante o saliente, funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"		
	El firewall/cortafuegos incorporado deberá ser totalmente administrable desde cliente o desde consola administrativa, así como deberá poseer modo de solución rápida a problemas comunes guiados intuitivamente desde la propia interfaz del producto.		
	Firewall/Cortafuegos incorporado deberá poseer facilidad para la definición de redes de confianza mediante parámetros de detección que faculten identificar si en realidad dispositivo protegido se encuentra en una red "segura" o bien se requiere un modo superior de protección en una red nueva y desconocida.		
	Incorpore IDS (Intrusion Detection System) de host para la prevención de acceso no autorizado al computador a nivel de capa de red,		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		
	Incorpore protección anti "BOTNETS", la cual faculte a la solución bloquear el acceso y comunicación a una red botnet así como alertar al usuario de dicha acción y anomalía detectada; funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		
	Incorpore Control de Vulnerabilidades a nivel de capa de red, el cual deberá inspeccionar y proteger a los protocolos más ampliamente utilizados SMB, RPC y RDP; evitando con dicho fin la propagación del malware, ataques de red dirigidos y la explotación de vulnerabilidades para las que un parche de seguridad aún no está disponible o ha sido desplegado, funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		
Antispam	Integre funcionalmente protección para la capa de transporte del correo electrónico provisionado por Servidor Microsoft Exchange en forma totalmente transparente, dicha funcionalidad deberá realizarla tanto para el correo saliente como el correo entrante sin requerir la instalación y/o modulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".		
	Integre funcionalmente protección Antimalware, Antispam, Anti-Phishing & Análisis mediante cloud sandboxing para todo correo electrónico enviado y/o recibido mediante Servidor Microsoft Exchange; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Integre funcionalmente protección antimalware para la base de datos embebida a Microsoft Exchange, de forma tal que pueda protegerse cada buzón de usuario e inclusive realizar análisis retrospectivo para los buzones de correo electrónico que pudiesen haber recibido código malicioso previo a la instalación de dicha solución de seguridad; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control"		
	Integre funcionalmente protección antimalware integrada directamente a la base de datos ocupada por Microsoft Exchange, que de forma tal proteja del envió/recepción de código malicioso inclusive cuando se ocupa portal web provisionado por Microsoft Exchange (OWA); no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control"		
	Integre funcionalmente protección a nivel de transporte para Microsoft Exchange, de forma tal que al menos pueda realizar lo siguiente:		
	• Filtrar correos electrónicos basado en el tipo de documento adjunto (identificador por tipo de ficheros)		
	• Filtrar correos electrónicos basado en el contenido del adjunto (identificador de ficheros por tipo y uso)		
	• Filtrar correos electrónicos basado en el contenido del cuerpo del mensaje (body message), de forma tal que pueda identificar características, texto o similar contenido en el mismo		
	• Filtrar correos electrónicos por tipo de extensión (filtrado de extensiones permitidas)		
	• Filtrar correos electrónicos por tamaño del mensaje		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	• Filtrar correos electrónicos que hayan sido enviados a múltiples usuarios (cadenas de mensaje)		
	• Delimitar cadenas de mensajes o bien identificar y bloquear por medio de contadores cualquier tipo de correo electrónico que encuadre en identificación de cadenas de mensajes (dirigido en forma específica una cantidad de usuarios por definir y totalmente variable, ej: 10, 30, 33 destinatarios en un solo mensaje).		
	Incorpore solución antispam a nivel ENDPOINT y posea filtrado para protocolo SMTP, POP3 & IMAP en forma transparente e integrada al producto sin requerir instalación de módulos y/o agentes en el computador; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".		
	Incorpore pluguin para el filtrado, análisis y clasificación antispam en los clientes de correo electrónico Microsoft Outlook, Windows Mail & Windows Live Mail; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".		
	Provea capacidad de generar listas blancas/negras para el filtrado del correo electrónico en la estación de trabajo final y en los clientes de correo electrónico indiciados como compatibles; dicha acción deberá de ser posible realizarse desde el propio producto y/o consola de administración, así como permitirá definir dominios y/o direcciones en cada uno de estos apartados.		
Web Filtering	Integre capacidad de Web Filtering basado en categorías, siendo posible definir políticas basadas en grupos de usuario y/o usuarios (tanto a nivel AD como también mediante autenticación local); no debe requerir de instalación y/o módulo		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".		
	Incorpore capacidad de Web Filtering mediante grupos de categorías, haciendo factible el agrupamiento de múltiples y diferentes categorías de inspección URL para una misma regla de navegación.		
	Faculte permitir y/o denegar el acceso URL estáticos mediante reglas configuradas en el Web Filtering.		
	Provea posibilidad de agrupamiento en políticas de filtrado URL, siendo factible sumar diferencialmente los accesos y/o denegaciones a fin de aplicar una política final de maquina o grupo de usuarios.		
	Integre capacidad para la generación de logs y sincronización de los mismos a consola corporativa, de acuerdo a cada una de las acciones tomadas en concordancia con la regla URL definida ya sea bloqueo o permisión según sea el caso; dicho log deberá contener toda la información detallada desde el URL bloqueado/permitido hasta el usuario/equipo detectado así como hora/fecha y descripción integra del evento; no debe requerir de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"		
	Integre capacidad Web Filtering sobre sitios URL que ocupen protocolo seguro (HTTPS); no debe requerir de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control".		
	Toda regla y/o política para el control URL, deberá poder ser fijada por horarios, días de la semana en particular y/o por usuarios en específico.		
Device Control	Incorpore capacidades de "Device Control" administrables ya sea localmente o en forma remota desde su consola administrativa; no debe requerir de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Programas -> Panel de Control".		
	Incorpore capacidades de "Device Control" avanzadas, con el fin de delimitar, denegar o permitir dispositivos portátiles y/o medios extraíbles tales como: • Dispositivos de almacenamiento USB • Dispositivos ópticos CD/DVD • Impresoras USB • Dispositivos de almacenamiento Firewire • Dispositivos Bluetooth • Tarjetas lectoras de memoria • Dispositivos de imagen • Modems • Puertos LPT/COM • Dispositivos portátiles (móviles)		
	Incorpore funciones avanzadas para el control de dispositivos siendo posible aplicar reglas con el fin de delimitar, denegar o permitir de acuerdo a las siguientes condiciones del dispositivo periférico conectado: • Marca • Modelo • Serie		
	Incorpore funciones avanzadas para el control dispositivos siendo capaz de asignar políticas de acuerdo a grupos de trabajo local o grupos dinámicos mediante un Directorio Activo; así mismo provea extensión de operación por usuario local y/o usuarios de un Directorio Activo.		
	Incorpore funciones avanzadas para el control de dispositivos mediante grupos de "dispositivos", siendo posible asignar reglas y/o directrices mediante grupos pre-establecidos de dispositivos con el fin de facilitar administración, así como el control adecuado de los dispositivos conectados a las estaciones de trabajo.		
	Toda regla y/o política para el control de dispositivos, deberá poder ser fijada por horarios, días de la semana en particular y/o por usuarios en específico.		

ESET Dynamic Threat Defense (Sandboxing En la Nube)

Protección	Descripción	CUMPLE	NO CUMPLE
Cloud Protection	Incorpore tecnología de detección en tiempo real basada en la nube, con el fin de prevenir ataques 0-Day y/o campañas de propagación de malware lanzadas globalmente; dicho alcance deberá garantizarse para correo electrónico, así como todo tipo de tráfico de red, tanto para reputación de archivos, así como vínculos URL.		
	Funcionalmente integración de tecnología "Cloud Protection" no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		
	Incorpore tecnología basada en la nube y en tiempo real, que permita al usuario operador del endpoint verificar la reputación de los procesos activos y de los archivos directamente desde la interfaz del programa o desde el menú contextual.		
	Incorpore tecnología sandboxing basada en la nube que integre al menos tres modelos de aprendizaje deep-learning (Deep Machine Learning) así como al menos seis modelos de clasificación para cada modelo Deep Machine Learning aplicado.		
	Incorpore capacidad para el envió manual de cualquier tipo de fichero para análisis mediante cloud sandboxing, asi como automáticamente y sin intervención alguna del usuario clasifique, detecte y/o elimine cualquier código malicioso nuevo o desconocido.		
	Incorpore tecnología en la nube para la detección de código nuevo y emergente, posibilitando detección del código malicioso y/o vínculo URL inclusive previo al lanzamiento de firmas antivirus de detección estándar.		

Protección	Descripción	CUMPLE	NO CUMPLE
	Incorpore tecnología "Antiphishing", de tal forma que prevenga al usuario de los intentos de adquirir contraseñas, datos bancarios y/o otra información sensible por parte de los sitios web falsos, haciéndose pasar por los legítimos; funcionalmente no debe requerir la instalación de módulos adicionales para tales fines, así como no deberá reflejarse como componente adicional en "Agregar/Quitar Programas".		

CONSOLA INTEGRADA PARA LA ADMINISTRACIÓN DE ESET-ENDPOINT SECURITY, ESET-DYNAMIC THREAT DEFENSE Y ESET MAIL SECURITY FOR EXCHANGE ENDPOINT SOLUTIONS G7 EDTD

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
Generalidades	Servidor de administración y consola administrativa deberá poder implementarse, así como proveer soporte multiplataforma compatible con al menos los siguientes sistemas operativos:		
	· Microsoft Windows Server 2019, 2016, 2012R2, 2012, 2008R2 y/o superior		
	· Microsoft Windows Server Core 2019, 2016, 2012R2, 2012, 2008R2 y/o superior		
	· Microsoft Windows 10, 8.1, 8 (CAL Microsoft puede limitar el soporte extendido, más sin embargo solución administrativa deberá poder instalarse y ser compatible con sistemas indicados).		
	RedHat, Debian, Ubuntu, Suse, Fedora & Mandriva así como la mayoría de distribuciones basadas en gestor de paquetes RPM y DEB.		
	Servidor de administración y consola administrativa deberá ofrecer compatibilidad para despliegue rápido mediante OVF; a fin de simplificar el despliegue de "Appliance Virtual" para el funcionamiento correcto de servidor administrativo de la solución adquirida.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Servidor de administración y consola administrativa deberá poder implementarse sobre plataforma Windows mediante un paquete todo en uno que incluya todos los elementos requeridos para instalación simplificada, así como ofrezca un fácil despliegue de solución administrativa; dicho paquete deberá incluir por defecto a los motores de base de datos, así como todo lo que integralmente requiere para su correcto funcionamiento el servidor y consola de administración.		
	Servidor de administración y consola administrativa deberá ofrecer compatibilidad con al menos las siguientes bases de datos:		
	· MySQL 5.5 o superior		
	· MS SQL Server 2008 R2 o superior		
	Servidor de administración y consola administrativa deberá ofrecer una consolidada y completa administración de los productos adquiridos, así como en su totalidad indicar el estado, configuraciones y políticas aplicadas de cada uno de los nodos internos ligados a dicha consola de administración.		
	Servidor de administración y consola administrativa deberá ofrecer posibilidad de integración con Active Directory, tanto para instalación remota de clientes, así como para autenticación local de administradores y roles de acceso a la misma.		
	Servidor de administración y consola administrativa deberá ofrecer diversos y variados roles de acceso mediante grupos de usuarios con el fin de definir niveles de acceso a administración de los diferentes recursos que dicha consola administrativa ofrezca a los administradores TI internamente.		
	Servidor de administración y consola administrativa deberá provisionar acceso web mediante servidor de aplicaciones JAVA.		
	Consola de administración deberá operar en su totalidad en modalidad web, así como integralmente deberá estar desarrollada y compilada sobre código JAVA.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Servidor de administración y consola administrativa deberá ofrecer posibilidad de segmentación para grandes redes mediante nodos de sincronización remota; de tal forma de facilitar la administración y sincronización de los clientes remotos, dichos nodos de sincronización podrán obrar como gestores de firmas, repositorios locales de instaladores, así como receptores de políticas y estados de los clientes locales.		
	Consola de administración deberá ser totalmente web, así como funcionalmente deberá ser compatible con cualquier navegador web tanto en sistemas operativos Microsoft, GNU/Linux, Mac OS y/o cualquier otro que a conveniencia pueda ocuparse para el acceso a dicha consola de administración.		
	Consola de administración web deberá garantizarse para al menos los siguientes navegadores en las versiones indicadas o superiores, sin requerir la instalación de algún plugin y/o complemento adicional del lado del cliente final:		
	· Firefox 20+		
	· Internet Explorer 10+		
	· Chrome 23+		
	· Safari 6+		
	· Opera 12+		
	Consola de administración web deberá ofrecer por completo administración para todos los productos ofertados independientemente del sistema operativo donde corre cliente o servidor, de forma tal que en su totalidad y absolutamente todos los productos sean administrados desde una sola interfaz web.		
	Consola de administración debe incorporar Dashboard accesibles desde cualquier navegador web y desde cualquier punto dentro o fuera de la red local; no debe requerir para dicha operación el uso de IIS o motor diferente al integrado nativamente por la solución.		
	Consola de Administración no deberá requerir de la existencia de un Dominio de Autenticación de Usuarios para su buen funcionamiento o como condicionante de operación; sin embargo, deberá permitir administrar clientes antivirus en distintos grupos de trabajo o multi-dominios ya existentes.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Consola de administración web no deberá requerir para su funcionamiento u operar sobre plataformas ASP, JSP o PHP.		
	Consola de administración deberá manejar múltiples tipos de Licencias de Software, en diferentes cantidades de equipos y fechas de expiración.		
	Consola de administración no deberá requerir el uso de MMC (Microsoft Management Console) para el funcionamiento de la misma o como requisito de instalación.		
	En términos de una correcta administración se requiere que una configuración establecida para un determinado cliente (ENDPOINT) pueda ser exportada, tanto desde la Consola de Administración, como desde el mismo cliente, para poder ser importada en otros clientes, de ser necesario.		
	Consola de administración deberá facultar instalación remota desatendida ya sea ocupando autenticación local o vía un directorio de autenticación, no importando si esta se realiza en dominio o en grupos de trabajo.		
	Consola y servidor de administración no deben requerir System Center Configuration Manager (SCCM), CM12, CM0, ConfigMgr, Configuration Manager o similar para uso de consola administrativa y/o servidor de administración; no debe figurar en especificaciones del fabricante (web/datasheets).		
	Servidor central de administración (consola/servidor) deberá ser compatible a nivel de almacenamiento de registros (logs) con base de datos MySQL y SQL Server; dicha compatibilidad deberá garantizar funcionamiento correcto con versiones “libre de pago” de dichas bases de datos (MySQL Community Edition & MS SQL Server Express).		
	Servidor central de administración deberá proveer compatibilidad con SYSLOG en forma nativa, de tal forma que los eventos ocurridos en los clientes puedan ser interpretados por un syslog server.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Consola y servidor de administración no deberán requerir Microsoft Message Queue como requisito para instalación y/o operación.		
	Consola/Servidor deberá provisionar doble factor de autenticación (2FA) para su interfaz web de administración; nativamente deberá ofertarse al menos en forma gratuita hasta cinco operadores y no deberá requerir de hardware/software que requiera pago o licenciamiento adicional.		
	Producto por adquirirse deberá funcionalmente ser compatible con consola de administración ESET Security Management Center ofreciendo integración para al menos las siguientes herramientas de centralización:		
	· CconnectWise Automate		
	· Datto RMM		
	· SolarWinds		
	· Ninja RMM		
	Consola de administración deberá funcionalmente ofrecer protección contra ataques de fuerza bruta, inactivando acceso a la fuente origen (IP) que ha causado afección y/o bien habilitando funcionalidades extendidas de seguridad por medio de un doble factor de autenticación.		
	Servidor de administración y consola administrativa deberá ofrecer una consolidada y completa administración de los productos adquiridos, así como en su totalidad indicar el estado, configuraciones y políticas aplicadas de cada uno de los nodos internos ligados a dicha consola de administración.		
	Servidor de administración y consola administrativa deberá ofrecer diversos y variados roles de acceso mediante grupos de usuarios con el fin de definir niveles de acceso a administración de los diferentes recursos que dicha consola administrativa ofrezca a los administradores TI internamente.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Servidor de administración y consola administrativa deberá ofrecer posibilidad de segmentación para grandes redes mediante nodos de sincronización remota; de tal forma de facilitar la administración y sincronización de los clientes remotos, dichos nodos de sincronización podrán obrar como gestores de firmas, repositorios locales de instaladores, así como receptores de políticas y estados de los clientes locales.		
	Consola de administración deberá ser totalmente web, así como funcionalmente deberá ser compatible con cualquier navegador web tanto en sistemas operativos Microsoft, GNU/Linux, Mac OS y/o cualquier otro que a conveniencia pueda ocuparse para el acceso a dicha consola de administración.		
	Consola de administración web deberá ofrecer por completo administración para todos los productos ofertados independientemente del sistema operativo donde corre cliente o servidor, de forma tal que en su totalidad y absolutamente todos los productos sean administrados desde una sola interfaz web.		
	Consola de administración debe incorporar Dashboard accesibles desde cualquier navegador web y desde cualquier punto dentro o fuera de la red local; no debe requerir para dicha operación el uso de IIS o motor diferente al integrado nativamente por la solución.		
	Consola de Administración no deberá requerir de la existencia de un Dominio de Autenticación de Usuarios para su buen funcionamiento o como condicionante de operación; sin embargo, deberá permitir administrar clientes antivirus en distintos grupos de trabajo o multi-dominios ya existentes.		
	En términos de una correcta administración se requiere que una configuración establecida para un determinado cliente (ENDPOINT) pueda ser exportada, tanto desde la Consola de Administración, como desde el mismo cliente, para poder ser importada en otros clientes, de ser necesario.		
	Se deberá provisionar método para la instalación remota desatendida ya sea ocupando autenticación local o vía un directorio de autenticación, no importando si esta se realiza en dominio o en grupos de trabajo.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Consola y servidor de administración no deben requerir System Center Configuration Manager (SCCM), CM12, CM0, ConfigMgr, Configuration Manager o similar para uso de consola administrativa y/o servidor de administración; no debe figurar en especificaciones del fabricante (web/datasheets).		
	Servidor central de administración (consola/servidor) deberá ser compatible a nivel de almacenamiento de registros (logs) con base de datos MySQL y SQL Server; dicha compatibilidad deberá garantizar funcionamiento correcto con versiones "libre de pago" de dichas bases de datos (MySQL Community Edition & MS SQL Server Express).		
	Servidor central de administración deberá proveer compatibilidad con SYSLOG en forma nativa, de tal forma que los eventos ocurridos en los clientes puedan ser interpretados por un syslog server basado en la nube.		
	Consola y servidor de administración no deberán requerir Microsoft Message Queue como requisito para instalación y/o operación		
	Consola/Servidor deberá provisionar doble factor de autenticación (2FA) para su interfaz web de administración; nativamente deberá ofertarse al menos en forma gratuita hasta cinco operadores y no deberá requerir de hardware/software que requiera pago o licenciamiento adicional.		
	Debe ser compatible con la solución actual.		
	Producto por adquirirse deberá ser totalmente gestionado, así como compatible con consola de administración interna ocupada para el efecto que por nombre se identifica como ESET Security Management Center, formalmente se deberá certificar compatibilidad desde sitio de fabricante donde se corrobore que el producto ofertado sea totalmente compatible con la consola de seguridad ocupada internamente.		
	Incorpore protección en tiempo real contra todo tipo de malware; incluyendo virus, gusanos, troyanos, spyware, phishing, rootkit, adware, riskware, keyloggers y/o otros códigos maliciosos nuevos y desconocidos.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Específicamente para dicho fin no deberá depender de que el Sistema Operativo del "ENDPOINT/Cliente" tenga las actualizaciones y Service Pack al día.		
	Incorpore protección contra virus boot, virus macros, virus residentes en RAM, virus de acción directa, virus encriptados, virus polimórficos, virus de FAT, etc.		
	Deberá integrar sandbox incorporado en el propio producto, con el objetivo de contener amenazas, emularlas, detectarlas y eliminarlas; dicha protección en particular deberá ser capaz de observar el comportamiento en tiempo real de cualquier binario en memoria operativa (RAM), siendo capaz de detectar basado en patrones de comportamiento & ML amenazas nuevas y desconocidas del tipo 0Day, APT's y/o cualquier tipo de código malicioso emergente.		
	Incorpore motor heurístico proactivo y preciso de tecnología avanzada, dicho motor debe ser propio y no de terceros fabricantes y/o colaboraciones externas ajenas a casa matriz.		
	Incorpore detección de virus en archivos compactados, sin importar el número de niveles de compresión, en los formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y/o otros.		
	Integralmente hablando producto instalado en el computador no deberá presentar fragmentación para su correcto funcionamiento (múltiples módulos instalados en el computador reflejados en programas instalados "Agregar/Quitar Programas" no serán aceptados, exceptuando únicamente al agente de conexión).		
	Deberá permitir importar o exportar configuraciones de clientes de manera fácil, vía archivos xml livianos y transportables.		
	Incorpore capacidad de poder enviar a los centros de soporte técnico las muestras de virus o códigos maliciosos, con la finalidad de que puedan ser analizados, y clasificados para su contingencia inmediata directamente desde la interfaz gráfica.		
	Incorpore capacidad de generar casos de soporte vía la interfaz gráfica de la solución.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Incorpore chequeo y control de Actualizaciones para Microsoft Windows, dicho control debe ser capaz de ser configurado para reportar diferentes niveles de actualización o desactivar el informe de las mismas.		
	Toda configuración a nivel de clientes, deberá poder ser posible realizarse desde consola administrativa y funcionalmente podrá gestionarse integralmente desde una única consola administrativa centralizada. Queda implícitamente descrito todos los productos adquiridos deberán administrarse desde una sola consola de administración, no importando el sistema operativo sobre el cual hayan sido implementados.		
	Incorpore compatibilidad nativa en su interfaz gráfica con dispositivos que integren tecnología TouchScreen.		
	Incorpore cache local de inspección a fin de mejorar el rendimiento en equipos virtualizados, explícitamente la cache de inspección local deberá validar si los ficheros fueron inspeccionados previamente por otro equipo en la red y en todo caso no forzar inspección local si el mismo es sano e inocuo al sistema a fin de acelerar el proceso de inspección. Dicha cache en aceleración de inspección antivirus/antimalware deberá de ser compatible con cualquier plataforma de virtualización, así como funcionalmente hablando no deberá requerir la instalación de ningún pluguin o complemento instalado y evidente desde "Control Panel -> Agregar o Quitar programas".		
	Solución a contratarse deberá provisionar capacidad para generar CD y/o USB Booteables, los cuales posean capacidad de análisis para la inspección de malware en máquinas que no cuenten con la protección de solución contratada o requieran del uso de los mismos con el fin de eliminar cualquier código malicioso, así mismo dichos medios deben poder ser actualizados vía Internet inmediatamente después del arranque desde los mismos.		
	Solución a contratarse deberá provisionar capacidad para generar CD y/o USB Booteables, los cuales deberán ofrecer como medio alternativo las siguientes herramientas de diagnóstico y asistencia técnica remota con proveedor o fabricante:		
	· Gparted		
	· MemTest86+		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	· Teamviewer		
	· Otras aplicaciones para recibir asistencia remota		
	· Otras		
	Solución a contratarse deberá cumplir con estándares AMTSO, identificables y validables en cada una de sus pruebas de evidencia técnica; de igual forma fabricante antivirus deberá figurar en el listado de miembros activos de AMTSO.		
	Solución a contratarse deberá incluir múltiples capas de seguridad, que deberán operar en forma conjunta y en su defecto tener capacidad de proteger independientemente si alguna de ellas no detecta en un momento dado el vector de ataque; dicho de otra forma, deberá garantizar proteger al endpoint final con diferentes métodos de protección y múltiples capas de seguridad comprobables según documentación de fabricante.		
	Incorpore protección a nivel Kernel, previniendo la desactivación y/o alteración por un tercero y/o código malicioso.		
	Incorpore auto-protección del núcleo y componentes de la suite de seguridad a nivel ASLR & DEP, así como funcionalmente no requiera de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”.		
	Incorpore protección en tiempo real contra cualquier alteración al estado del kernel antivirus, imposibilitando detenerlo o dejarlo inoperativo para protección del computador donde ha sido implementado.		
	Integre protección nativa de aprendizaje automático, la cual deberá incluir mecanismos de simulación/detección mediante redes neurales y al menos seis algoritmos de clasificación integrados, dicho módulo de protección deberá coadyuvar en la detección de cualquier tipo de código malicioso nuevo y/o desconocido; así como funcionalmente no debe requerir de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Deberá integrar protección nativa a nivel UEFI que permita comprobar y aplicar seguridad para el entorno previo al inicio y arranque del equipo, dicho modulo deberá detectar componentes maliciosos en el firmware (UEFI/BIOS); funcionalmente no debe requerir de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".		
	Incorpore capacidad de protección por contraseña de acceso al propio motor antivirus, a fin de que no pueda ser alterada configuración de la propia solución y/o alteración al estado de protección del computador.		
	Instalación de producto podrá realizarse tanto localmente como remotamente desde su consola administrativa; en el término local se entiende se requiere pre compilación de un paquete todo-en-uno para la instalación del producto el cual contenga las pre configuraciones y niveles de seguridad básicos aplicables a la estación de trabajo, así mismo incorpore en un solo paso la unión y sincronización a consola administrativa.		
	Comunicación entre clientes administrados (ENDPOINTS) y servidor de administración deberá realizarse mediante conexión SSL cifrada; dicha conexión deberá ser evidente y descrita en el log de estado del agente de conexión mediante cualquier navegador web para fines de validación o auditoria.		
	Agente de conexión deberá provisionar log transaccional de referencia, así como en forma simultánea deberá mostrar su estado de conexión y descripción general de sincronizaciones a servidor administrativo; dicho log deberá ser accesible desde cualquier navegador web y en forma dinámica deberá variar en forma automática a fin de evidenciar cualquier problema de comunicación o falla de transferencia y/o comunicación cifrada en la línea del tiempo.		
	Agente de conexión deberá reportar en forma precisa todo software de terceros y/o fabricante contratado ubicado en el computador que figure como instalado en el equipo donde ha sido instalado.		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	Agente de conexión deberá reportar en forma precisa todo hardware instalado en el computador donde ha sido instalado, reportando con precisión todo lo referente al hardware presente.		
	Agente de conexión deberá soportar instalación de software de terceros, no delimitando e incluyendo cualquier aplicativo (EXE) que desee ejecutarse o instalarse en los computadores administrados.		
	Solución a contratarse requiere soporte técnico directo del fabricante y que este pueda prestarlo localmente en formato 24x7x365; el mismo en sus modalidades deberá garantizarse ya sea en forma presencial, remota, chat en línea, correo electrónico y/o vía telefónica mediante número local; en caso que la empresa adjudicada por alguna razón no pueda proporcionarlo.		
	Nativamente consola de administración deberá poseer soporte para equipos y/o servidores clonados sean estos físicos o virtuales, de forma tal que el identificador por disco o volumen de disco no constituya un problema para identificar individualmente cada equipo administrado.		
	Deben incluirse medias de Instalación originales provistas por el fabricante, evidenciables mediante certificado de originalidad provisto por el fabricante y entregado con las mismas.		
	Ofertante deberá demostrar experiencia comprobable con respecto al software ofertado para implementación, administración y soporte técnico dentro del territorio nacional que rige este evento para al menos cinco años calendario; en resguardo a los bienes de la institución, así como garantía de cumplimiento del ofertante, no se aceptaran ofertas que no proporcionen la información solicitada y/o bien no presenten las pruebas que así lo demuestren.		
	Ofertante deberá demostrar poseer experiencia comprobable para la implementación, administración y soporte técnico en al menos dos clientes que sean igual o superiores a la cantidad total de nodos computacionales que rige este evento; dicho requerimiento será admitido como válido en formalidad únicamente para referencias dentro de territorio nacional, no se aceptaran referencias del extranjero o que no coincidan en su totalidad con el		

Protección	Especificación Técnica	CUMPLE	NO CUMPLE
	producto ofertado, en resguardo a los bienes de la institución, así como garantía de cumplimiento del ofertante, no se aceptaran ofertas que no proporcionen la información solicitada y/o bien no presenten las pruebas que así lo demuestren.		
	Ofertante deberá garantizar en totalidad de forma y por escrito que todo tipo de soporte técnico solicitado por esta institución ya sea con el propio ofertante y/o con el fabricante en cualesquiera de sus modalidades 24x7x365 sea totalmente gratuito, así como garantice en su totalidad no aplique ninguna restricción por horas de servicio o similar.		
	Ofertante deberá demostrar mediante documento oficial de fabricante, el mismo es un proveedor autorizado para el territorio nacional de sus productos; en caso fabricante no posea oficinas locales dentro del territorio nacional deberá indicarse como no cumplimiento al requerimiento específico sobre dicho aspecto, así como deberá considerarse todo documento que ampare al ofertante como proveedor oficial de solución ofertada cumpla con protocolo de ley para la nacionalización de documentos procedentes del extranjero.		

CONDICIONES PARA LA RECEPCIÓN

- La recepción del licenciamiento deberá ser inmediata, después de la adjudicación. El licenciamiento es en línea y la empresa adjudicada deberá asegurarse del registro de las mismas en los servidores del fabricante a nombre del Poder Judicial de Honduras.

- El suministro de "LICENCIAS (RENOVACIÓN ESET ENDPOINT PROTECCION ADVANCED, ESET MAIL SECURITY FOR EXCHANGE ENDPOINT SOLUTIONS G7 EDTD, SANDBOXING EN LA NUBE –ESET DYNAMIC THREAT DEFENSE,)", con disponibilidad de entrega inmediata.

FASE IV. EVALUACIÓN TÉCNICA FÍSICA:

La información técnica solicitada debe ajustarse a la Evaluación Técnica escrita en la Fase III de este pliego de condiciones.

Solamente las ofertas que superen estas fases pasarán a la siguiente Fase, las ofertas que no la superen serán descalificadas.

FASE V, EVALUACIÓN ECONÓMICA: Descripción de documentación de la oferta económica

Descripción	TIPO DE LICENCIA	Producto	Valor Unitario L	Impuesto Sobre Venta	Sub-Total	Total L
Renovación de Licencia de antivirus ESET ENDPOINT Protection Advanced.	ESET ENDPOINT PROTECTION ADVANCED	A) Protection para Endpoints- ESET Endpoint Security, Antivirus y Antispyware.	L	L	L	L
		B) Sandboxing en la nube- ESET Dynamic Threat Defense	L	L	L	L
		C) Protection para Correos Electrónicos - ESET Mail Security For Exchange Endpoint Solutions G7 Edtd	L	L	L	L
Total, Global						**L**

IO-12 ERRORES U OMISIONES SUBSANABLES

Podrán ser subsanados los defectos u omisiones contenidas en las ofertas, en cuanto no impliquen modificaciones del precio, objeto y condiciones ofrecidas.

En caso de haber discrepancia entre precio expresado en letras y en cifras serán válidos los establecidos en letras, asimismo, si hubiera diferencia entre el precio unitario y el precio total se considerará el primero.

La comisión de evaluación podrá corregir los errores aritméticos que se detecten durante la evaluación de las ofertas, debiendo notificar al oferente. Quien deberá aceptarlas a partir de la recepción de la notificación o su oferta será descalificada.

El valor y el plazo de la Garantía de Mantenimiento de Oferta no serán subsanables y lo establecido en el artículo 131 del Reglamento de la Ley de Contratación del Estado.

IO-13 ADJUDICACIÓN DEL CONTRATO

La adjudicación del contrato se hará al oferente que, cumpliendo las condiciones de participación, incluyendo su solvencia e idoneidad para ejecutar el contrato, presente **la oferta de precio más bajo** o se considere la más económica o ventajosa y por ello mejor calificada, de acuerdo con criterios objetivos establecidos.

IO-14 NOTIFICACIÓN DE ADJUDICACION DEL CONTRATO

La resolución que emita el órgano responsable de la contratación adjudicando el contrato, será notificada a los oferentes y publicada, dejándose constancia en el expediente. La publicación deberá incluir como mínimo la siguiente información.

a) El nombre de la entidad
b) Una descripción de las mercancías o servicios incluidos en el contrato
c) El nombre del Oferente ganador
d) El valor de la Adjudicación.

Si la adjudicación no se notifica dentro del plazo de la vigencia de las ofertas, los proponentes podrán retirar sus ofertas sin responsabilidad de su parte.

IO-15 FIRMA DE CONTRATO

- Se procederá a la firma del contrato dentro de los treinta (30) días calendario siguiente a la notificación de la adjudicación, mismo que se formalizará mediante suscripción del documento correspondiente, entre la autoridad competente y quien ostente la Representación Legal del adjudicatario. [3]

- Antes de la firma del contrato, el oferente ganador deberá dentro de los cinco (05) días calendario presentar los siguientes documentos:

1. Constancia original de la Procuraduría General de la República, de no tener juicios pendientes con el Estado de Honduras. Original o copia autenticada de la solvencia vigente del oferente (Sistema de Administración de Rentas) Constancia de Solvencia Fiscal.

2. Constancia de inscripción en el Registro de Proveedores y Contratistas del Estado, extendida por la ONCAE (solo en caso de haber presentado constancia de estar en trámite en el momento de presentar la oferta).
3. Constancia de solvencia por el Instituto Hondureño de Seguridad Social (IHSS).

Si el oferente no acepta la adjudicación, no firma el contrato o no presenta la documentación detallada dentro del plazo establecido, por causas que le fueren imputables a él, perderá todos los derechos adquiridos en la adjudicación y dará lugar a la ejecución de la Garantía de mantenimiento de la oferta. Se procederá a adjudicar el contrato al ofertante que haya presentado la segunda mejor oferta evaluada, la más baja y ventajosa y así sucesivamente.

[3] Para contratos bajo Licitación Pública la LCE requiere treinta (30) días para la formalización del contrato

SECCION II - CONDICIONES DE CONTRATACION

CC-01 ADMINISTRADOR DEL CONTRATO

El Poder Judicial nombrará un Administrador del Contrato, quien será responsable de verificar la buena marcha y cumplimiento de las obligaciones contractuales, que entre sus funciones tendrá las siguientes:

a. Verificar que la Dirección Administrativa emita la correspondiente Orden de Compra.
b. Dar seguimiento a la entrega final;
c. Emitir acta de recepción final;
d. Documentar cualquier incumplimiento del Contratista.
e. Interpretación del contrato.
f. El Poder Judicial designará un Supervisor de la Dirección de Infotecnología, quien será el encargado de la administración del contrato y de vigilar la buena marcha de lo estipulado en el mismo y sobre todas o algunas de las funciones siguientes:
g. Decidir sobre todas y cada una de las preguntas que puedan surgir acerca de la calidad y aceptabilidad del suministro solicitado.
h. Velar por el estricto cumplimiento del contrato.
i. Interpretar las especificaciones
j. Aprobar la calidad del servicio, objeto del contrato de suministro.
k. Inspeccionar y recomendar la aceptación final del servicio, objeto del contrato de suministro y, según sea el caso, de sus partes.
l. Tramitar ante el Poder Judicial, las Órdenes de Compra o Modificaciones al Contrato.
m. Presentar su decisión por escrito dentro de un tiempo prudencial, acerca de los reclamos, desacuerdos y otros asuntos en relación con la interpretación del contrato.
n. Participar en la recepción total del servicio y recomendar la suscripción de las actas de recepción respectivas.
o. Dar seguimiento a la ejecución del contrato por parte a la Dirección Administrativa.

CC-02 PLAZO CONTRACTUAL

El contrato estará vigente desde ***su otorgamiento hasta cumplir la vigencia de la prestación del servicio***.

El contrato será por un (1) año y la vigencia o plazo de duración del licenciamiento por dos (2) años, con un periodo de cobertura desde el 31 enero, 2023 al 31 de enero, 2025.

Iniciando el periodo de renovación con el vencimiento del licenciamiento del contrato actual para “ESET ENDPOINT PROTECCION ADVANCED, ESET MAIL SECURITY FOR EXCHANGE ENDPOINT SOLUTIONS G7 EDTD, SANDBOXING EN LA NUBE –ESET DYNAMIC THREAT DEFENSE,)”.

De conformidad al Artículo 360 de la Constitución de la República, los contratos que el Estado celebra para la ejecución de obras públicas, adquisición de suministros y servicios, de compra, venta o arrendamiento de bienes, deberán ejecutarse previa licitación, concurso o subasta de conformidad con la Ley.

La contratación para el ejercicio fiscal posterior para el que se contrata, deberá seguir el procedimiento establecido en el Artículo 15 de la Ley Orgánica del Presupuesto, contenida en el Decreto N. 83-2004; es decir que el anteproyecto de presupuesto de esta institución presentado ante la Secretaria de Finanzas; para aprobación posterior del Congreso Nacional, para el o los años fiscales subsiguientes debe consignar de manera expresa la información sobre los bienes y servicios hasta por su monto total y el importe para cada una de las anualidades. Por lo que se deberá de contar para el segundo año de contrato con la Disponibilidad Presupuestaria correspondiente para el mismo.

El pago se realizará en un solo pago según lo dispuesto por la Dirección Administrativa del Poder Judicial y conforme a lo establecido en las Especificaciones Técnicas Generales de estas Bases de Licitación.

CC-03 CESACIÓN DEL CONTRATO

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

CC-04 LUGAR DE ENTREGA DEL SUMINISTRO

La entrega del servicio se hará en:

- La recepción del suministro objeto de la presente licitación, se realizará en la Dirección de Infotecnología, edificio principal del Poder Judicial, en la ciudad de Tegucigalpa, M.D.C., suscribiendo un Acta de Recepción, el número del producto autorizado se recibe electrónicamente a través del correo oficial del Poder Judicial, misma que deberá ser entregada de forma inmediata después de la adjudicación.

CC-05 PLAZO Y CANTIDADES DE ENTREGA DEL SUMINISTRO

El Proveedor que resulte adjudicado debe contar con disponibilidad inmediata para suministrar a la Dirección de Infotecnología del Poder Judicial, las 5,000 licencias del software antivirus ESET ENDPOINT PROTECCION ADVANCED, ESET MAIL SECURITY FOR EXCHANGE ENDPOINT SOLUTIONS G7 EDTD, SANDBOXING EN LA NUBE –ESET DYNAMIC THREAT DEFENSE, en una sola entrega.

CC-06 PROCEDIMIENTO DE RECEPCIÓN

CONDICIONES PARA LA RECEPCIÓN

- La recepción del licenciamiento deberá ser inmediata, después de la adjudicación, el licenciamiento es en línea y la empresa adjudicada deberá asegurarse del registro de las mismas en los servidores del fabricante a nombre del Poder Judicial de Honduras.

- El suministro de "LICENCIAS (RENOVACIÓN ESET ENDPOINT PROTECCION ADVANCED, ESET MAIL SECURITY FOR EXCHANGE ENDPOINT SOLUTIONS G7 EDTD, SANDBOXING EN LA NUBE –ESET DYNAMIC THREAT DEFENSE,)", con disponibilidad de entrega inmediata.

CC-07 GARANTÍAS

Se aceptarán solamente fianzas y garantías bancarias emitidas por instituciones debidamente autorizadas y cheques certificados.

Todas las garantías contendrán indefectiblemente la Cláusula Obligatoria siguiente: "***LA PRESENTE GARANTÍA/FIANZA SERA EJECUTADA POR EL MONTO TOTAL DE LA MISMA A SIMPLE REQUERIMIENTO DEL BENEFICIARIO, ACOMPAÑADA DE UNA RESOLUCION FIRME DE INCUMPLIMENTO, SIN NINGUN OTRO REQUISITO, PUDIENDO REQUERIRSE EN CUALQUIER MOMENTO DENTRO DEL PLAZO DE VIGENCIA DE LA GARANTIA/FIANZA. LA PRESENTE GARANTIA/FIANZA EMITIDA A FAVOR DEL BENEFICIARIO CONSTITUYE UNA OBLIGACION SOLIDARIA, INCONDICIONAL, IRREVOCABLE Y DE EJECUCION AUTOMATICA; EN CASO DE CONFLICTO ENTRE EL BENEFICIARIO Y EL ENTE EMISOR DEL TITULO, AMBAS PARTES SE SOMETEN A LA JURISDICCION DE LOS TRIBUNALES DE LA REPUBLICA DEL DOMICILIO DEL BENEFICIARIO. LA PRESENTE CLAUSULA ESPECIAL OBLIGATORIA PREVALECERA SOBRE CUALQUIER OTRA CONDICIÓN.***"

a) GARANTÍA DE MANTENIMIENTO DE OFERTA.

- Los oferentes deben acompañar a su oferta una Garantía de Mantenimiento de Oferta en moneda Nacional equivalente al Dos por ciento (2%) del valor ofertado. Esta garantía debe ser expedida a nombre del Poder Judicial y podrá consistir en una garantía bancaria, fianza o cheque certificado (mismo que se hará efectivo en caso de incumplimiento) expedida por el sistema Bancario Nacional o Aseguradora del país, pagadero a la vista, para proteger al Poder Judicial contra el riesgo de incumplimiento por parte del oferente de la propuesta presentada.
- La garantía presentada tendrá una vigencia mínima de ciento setenta (170) días calendario a partir de la fecha de apertura privada de ofertas, y será devuelta a los licitantes dentro de los (60) sesenta días calendario siguientes a la fecha en que se firme el contrato con el licitante a quien se adjudique el mismo. Artículo 99 de la Ley de Contratación del Estado. (Art. 117

R.L.C.E)

b) GARANTÍA DE CUMPLIMIENTO DE CONTRATO

- El proveedor deberá presentar la Garantía de Cumplimiento de contrato al momento de suscribir el mismo. Esta garantía deber ser expedida a nombre del Poder Judicial y podrá consistir en una garantía bancaria, fianza o cheque certificado (mismo que se hará efectivo en caso de incumplimiento) expedida por el sistema Bancario Nacional o Aseguradora del Pais, pagadero a vista, para proteger al Poder Judicial contra el riesgo de incumplimiento por parte del oferente de la propuesta presentada.

- La Garantía de Cumplimiento del contrato deberá ser presentada en original.

- Valor: La garantía de cumplimiento del contrato deberá ser al menos, por el valor equivalente al quince por ciento (15%) de monto contractual.

- Vigencia: La garantía de cumplimiento del contrato deberá estar vigente hasta al menos treinta (30) días posteriores a la fecha de vencimiento de la vigencia del contrato.

- Para la correcta ejecución del Contrato, la Garantía de Cumplimiento debe presentarse al momento de la emisión de la orden de compra por parte de la Dirección Administrativa. Esta presentación debe coordinarse entre el Contratista y la Dirección Administrativa a través del Supervisor del Contrato. Así mismo deberá presentarse la Declaración Jurada emitida por la Institución Garante que extendió esta Garantía de Cumplimento según lo dispuesto en el artículo 241 y 242 del Reglamento de Ley de Contratación del Estado. La garantía de cumplimento deberá ser sustituida dentro de lo diez (10) días calendario, posteriores a la formalización del contacto.

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

c) GARANTIA DE BUEN SUMINISTRO

El oferente favorecido otorgara a favor del Poder Judicial una garantía equivalente al cinco por ciento (5%) del monto del contrato, por los vicios o defectos del suministro, conforme al Artículo 104 de la Ley de Contratación del Estado. Esta garantía entrará en vigencia a partir de la fecha de la recepción final, con una duración de 24 meses, después de finalizado el Suministro, Mediante esta garantía el Contratista se compromete a reponer o reparar por su cuenta cualquier defecto y/o fallas ocasionadas por deficiencias en materiales, mano de obra, equipamiento, vicios ocultos y por cualesquier otros aspectos que fueran imputables a él.

Asimismo, se compromete a subsanar los daños y perjuicios ocasionados al Poder Judicial o a terceros que se deriven de las causas antes indicadas, excepto los ocasionados por fuerza mayor o caso fortuito debidamente comprobados.

Esta garantía debe ser expedida a nombre del Poder Judicial, en moneda nacional y podrá consistir en Garantía Bancaria o Póliza, expedida por el sistema bancario nacional o aseguradora de este país.

- **AFECTACIÓN DE LAS GARANTÍAS**

Si hubiera reclamos al Contratista por incumplimiento, de sus obligaciones y estuviere próximo a expirar el plazo de una garantía, el Poder Judicial, afectara la Garantía ante la entidad garante, quedando la garantía desde ese momento afectada al reclamo, sin que pueda alegarse luego expiración del plazo.

- **RECLAMOS**

Cualquier reclamo en etapa de ejecución del Contrato que el Poder Judicial formalice y no sea atendido en un plazo máximo de **dos (2) días hábiles**, y no se logre concertar un acuerdo conciliatorio entre las partes, dará lugar a la rescisión del contrato o ejecución de la Garantía de Cumplimiento.

- **EJECUCIÓN DE LA GARANTÍA DE CUMPLIMIENTO DE CONTRATO**

Si el proveedor diere indicios racionales de incumplimiento de todos o algunos de los compromisos estipulados en el contrato, en el pliego de condiciones o en su oferta, el Poder Judicial procederá a afectar y luego ejecutar su Garantía de Cumplimiento de Contrato. Y no se aceptará su participación en futuros procesos de contratación realizados para este fin.

CC-08 FORMA DE PAGO

Se realizará un solo pago, una vez recibido el suministro objeto de la presente licitación en moneda nacional (Lempiras). El proveedor requerirá el pago al Poder Judicial y adjuntará a la solicitud una factura que describa los bienes y/o servicios entregados, la correspondiente Acta de Recepción y Recibo a nombre del Poder Judicial.

El pago se realizará a través de la Dirección Administrativa y de conformidad con los procedimientos establecidos por normas administrativas vigentes y según lo especificado en el calendario de entregas.

CC-09 MULTAS

Cuando el contratista incurriere en mora en el cumplimiento de sus obligaciones contractuales por causas imputables al mismo, se le impondrá el pago de una multa por cada día de retraso, de conformidad lo establecido en las vigentes Disposiciones Generales del Presupuesto General de Ingresos y Egresos de la República. El Poder Judicial efectuará un seguimiento de acuerdo al plazo de entrega, el incumplimiento del mismo dará lugar a la aplicación del Artículo 72 de la Ley de Contratación del Estado que estará en relación con Articulo 76 de las Disposiciones del Presupuesto General de Ingresos y Egresos de la República para el ejercicio fiscal 2022, que expresa: “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 punto treinta y seis por ciento (0.36%), así como la multa pecuniaria aplicable por cada día de retraso, en relación con el monto total del saldo del contrato por el incumplimiento del

plazo y la misma debe especificarse tanto en el pliego de condiciones como en el contrato de Construcción y Supervisión de Obras Públicas, es decir debe estar establecida en todo contrato y toda orden de compra. Esta misma disposición se debe aplicar a todos los contratos de bienes y servicios que celebren las Instituciones del Sector Público".

CC-10 LICITACIÓN DESIERTA O FRACASADA

El Poder Judicial, en aplicación al Art. 57 de la Ley de Contratación del Estado y 172 de su Reglamento se reserva el derecho de declarar desierta la Licitación cuando no se hubieren presentado ofertas o no se hubiere satisfecho el mínimo de oferentes previstos en el pliego de condiciones y la declarara fracasada en los casos siguientes:

- Cuando se hubiere omitido en el procedimiento algunos de los requisitos esenciales establecidos en la Ley o en sus disposiciones reglamentarias y a los intereses del Poder Judicial.
- Cuando las ofertas no se ajusten a los requisitos esenciales establecidos en el Reglamento de la Ley y en el Pliego de condiciones.
- Cuando se comprobare que ha existido colusión.
- Ofertas por precios considerablemente superiores al presupuesto base estimado por el Poder Judicial.
- Cuando antes de decidir la adjudicación, sobrevinieren motivos de Fuerza mayor debidamente comprobados que impidieran su conclusión.
- Declarada desierta o fracasada la licitación se procederá a una nueva Licitación.

CC-11 FORMALIZACIÓN DE LOS CONTRATOS

La formalización de los contratos no requerirá otorgamiento de Escritura Pública, ni uso de papel sellado y timbres, y se entenderán perfeccionados a partir de su suscripción.

El contrato se suscribirá dentro de los treinta (30) días calendario siguientes a la notificación de la adjudicación, si el oferente a quien se le adjudicó el contrato no lo acepta o no lo formaliza por causas que le fueren imputables, dentro del plazo antes señalado, quedará sin valor ni efecto la adjudicación y la Administración hará efectiva la garantía de mantenimiento de oferta. Si así ocurriere, el órgano responsable de la contratación podrá adjudicar el Contrato al oferente que resultó en segundo lugar y si esto no fuera posible por cualquier motivo, al oferente que resultó en tercer lugar y así sucesivamente, sin perjuicio de que el procedimiento se declare fracasado cuando las otras ofertas no fueren satisfactorias para la Administración.

Una vez formalizado el contrato, el oferente favorecido se compromete a sustituir en un plazo no mayor a diez (10) días calendario, la garantía de mantenimiento de oferta, salvo causa justificada, por una garantía de cumplimiento equivalente al quince por ciento (15%) del valor total de la oferta y servirá para garantizar que el contratista entregue el suministro cumpliendo con todas las condiciones estipuladas en el contrato, la cual deberá tener una vigencia de tres (3) meses después del plazo previsto para la entrega del servicio.

Si el oferente favorecido no presenta la Garantía de Cumplimiento en el plazo mencionado en el párrafo anterior, el Poder Judicial a través de la Administración afectará la Garantía de Mantenimiento de Oferta; salvo causa debidamente justificada, debiendo informar oportunamente a la administración los inconvenientes sufridos, a efecto de que esta conceda un plazo mayor al estipulado, quedando a criterio de la Dirección Administrativa el otorgamiento de un nuevo plazo para su presentación.

Los derechos y obligaciones previstos en el contrato serán efectivos solamente a partir de su legalización por parte del Poder Judicial.

A los oferentes no favorecidos con la adjudicación, se les devolverá su respectiva garantía de mantenimiento de Oferta, dentro de los sesenta (60) días hábiles siguientes a la fecha en que se firme el contrato con el adjudicatario.

El órgano encargado de velar por la correcta ejecución del contrato será responsable de que las garantías se constituyan oportunamente por el Contratista, y que cumplan los fines para los que fueron expedidas. En consecuencia, si hubiese reclamos pendientes estando próximo a expirar cualquier garantía que responda por obligaciones del Contratista, la autoridad competente notificará este hecho a la empresa afianzadora o garante, quedando desde ese momento la garantía afecta al resultado de los reclamos.

CC-12 RESCISIÓN DE CONTRATO

Facultad que tiene el Poder Judicial y el contratista para rescindir el contrato si existe incumplimiento grave de alguna de las partes de conformidad con lo estipulado en la Ley de Contratación del Estado y su Reglamento, así como el Decreto N° 30-2022 publicado el 08 de abril de 2022 en la Gaceta, Diario Oficial de la República de Honduras bajo el numero 35,894 Articulo N°78 del Presupuesto General de Ingresos y Egresos de la República, Ejercicio Fiscal 2022 el cual expresa lo siguiente: 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 al 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 menores a los gastos proyectados y en caso de necesidades imprevistas o de emergencia.

Lo dispuesto en este Artículo debe estipularse obligatoriamente en los pliegos de condiciones, bases de Licitación, términos de referencia u otros documentos previos a la celebración del contrato y en el contrato mismo del Sector Público.

CC-13 LEYES Y REGLAMENTOS APLICABLES

Son aplicables en ésta licitación, el presente documento contentivo del pliego de condiciones, la Constitución de la República, Ley de Contratación del Estado y su Reglamento, Ley de Procedimientos Administrativos, Disposiciones Generales del Presupuesto General de Ingresos y egresos de la Republica vigente, Reglamento de Ejecución Presupuestaria del Poder Judicial, y demás leyes aplicables a la materia, conforme a lo establecido en el Artículo 14 del Reglamento de la Ley de Contratación del Estado.

SECCION III - ESPECIFICACIONES TECNICAS

A continuación, se presenta la descripción técnica del material objeto de adquisición:

No	TIPO DE LICENCIA	Especificaciones Técnicas Incluye	Descripción	CANTIDAD
1	ESET ENDPOINT PROTECTION ADVANCED	A) Protection para Endpoints-ESET Endpoint Security, Antivirus y Antispyware.	Protección Avanzada en múltiples niveles para PC, Smartphones y máquinas virtuales. Elimina todos los tipos de amenazas, incluyendo virus, rootkits, gusanos y spyware	5,000
		B) Sandboxing en la nube-ESET Dynamic Threat Defense	Protección Mejorada contra ransomware y amenazas 0-day a través del sandboxing en la nube	
		C) Protection para Correos Electrónicos - ESET Mail Security For Exchange Endpoint Solutions G7 Edtd	Bloquean spam y malware a nivel del servidor, antes de que lleguen a las casillas de correo de los usuarios	

ALCANCE

El alcance de la renovación del licenciamiento del software antivirus es aplicable para todos los equipos informáticos conectados a la red tecnológica y distribuidos a nivel nacional en cada sede judicial. Incluye computadoras de usuarios, servidores, y las diferentes plataformas tecnológicas virtuales del Poder Judicial.

PROTECTION PARA ENDPOINTS-ESET ENDPOINT SECURITY, ANTIVIRUS Y ANTISPYWARE.

Protección	Especificación Técnica
Sistemas Operativos Compatibles	Incorpore garantía de compatibilidad extendida para sistemas operativos 32bits y 64bits:
	- Microsoft Windows® 11,10,8.1, 8, 7 SP1 y/o superior
	- Microsoft Windows Server 2019,2016,2012R2,2012,2008R2,2008 y/o superior
	- Microsoft Windows Server Core 2019, 2016, 2012R2, 2012, 2008R2, 2008 Core y/o superior
	- OS X 10.6 y/o superior
	- RedHat, Debian, Ubuntu, Suse, Fedora & Mandriva así como la mayoría de distribuciones basadas en gestor de paquetes RPM y DEB
	Incorpore garantía de compatibilidad extendida para las siguientes versiones de servidores de correo electrónico:
	- Microsoft Exchange Server 2019, 2016, 2013, 2010, 2007
	Licenciamiento otorgado deberá poseer garantía y cobertura sobre los sistemas operativos indicados como requeridos, se acepta un solo y único lote de licenciamiento que involucre a todos los sistemas indicados; puntualmente deberá ocuparse una única clave de activación, llave o similar para todos los productos contratados e indicados como compatiblemente requeridos.
	Licenciamiento adquirido en su totalidad deberá poder ser administrado por una única consola de administración, todos los productos adquiridos para los sistemas operativos indicados como compatibles deberán poderse administrar integralmente desde una única consola validada e implementada en la red interna corporativa.
Aspectos Generales	Incorpore protección en tiempo real contra todo tipo de malware; incluyendo virus, gusanos, troyanos, spyware, phishing, rootkit, adware, riskware, keyloggers y/o otros códigos maliciosos nuevos y desconocidos. Específicamente para dicho fin no deberá depender de que el Sistema Operativo del "ENDPOINT/Cliente" tenga las actualizaciones y Service Pack al día
	Incorpore protección contra virus boot, virus macros, virus residentes en RAM, virus de acción directa, virus encriptados, virus polimórficos, virus de FAT, etc.
	Deberá integrar sandbox incorporado en el propio producto, con el objetivo de contener amenazas, emularlas, detectarlas y eliminarlas; dicha protección en particular deberá ser capaz de observar el comportamiento en tiempo real de cualquier binario en memoria operativa (RAM), siendo capaz de detectar basado en patrones de comportamiento & ML amenazas nuevas y desconocidas del tipo 0Day, APT's y/o cualquier tipo de código malicioso emergente.

Protección	Especificación Técnica
	Incorpore motor heurístico proactivo y preciso de tecnología avanzada, dicho motor debe ser propio y no de terceros fabricantes y/o colaboraciones externas ajenas a casa matriz.
	Incorpore detección de virus en archivos compactados, sin importar el número de niveles de compresión, en los formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y/o otros.
	Integralmente hablando producto instalado en el computador no deberá presentar fragmentación para su correcto funcionamiento (múltiples módulos instalados en el computador reflejados en programas instalados "Agregar/Quitar Programas" no serán aceptados, exceptuando únicamente al agente de conexión).
	Deberá permitir importar o exportar configuraciones de clientes de manera fácil, vía archivos xml livianos y transportables.
	Incorpore capacidad de poder enviar a los centros de soporte técnico las muestras de virus o códigos maliciosos, con la finalidad de que puedan ser analizados, y clasificados para su contingencia inmediata directamente desde la interfaz gráfica.
	Incorpore capacidad de generar casos de soporte vía la interfaz gráfica de la solución.
	Incorpore chequeo y control de Actualizaciones para Microsoft Windows, dicho control debe ser capaz de ser configurado para reportar diferentes niveles de actualización o desactivar el informe de las mismas.
	Toda configuración a nivel de clientes deberá poder ser posible realizarse desde consola administrativa y funcionalmente podrá gestionarse integralmente desde una única consola administrativa centralizada. Queda implícitamente descrito todos los productos adquiridos deberán administrarse desde una sola consola de administración, no importando el sistema operativo sobre el cual hayan sido implementados.
	Incorpore compatibilidad nativa en su interfaz gráfica con dispositivos que integren tecnología TouchScreen.
	Incorpore cache local de inspección a fin de mejorar el rendimiento en equipos virtualizados, explícitamente la cache de inspección local deberá validar si los ficheros fueron inspeccionados previamente por otro equipo en la red y en todo caso no forzar inspección local si el mismo es sano e inocuo al sistema a fin de acelerar el proceso de inspección. Dicha cache en aceleración de inspección antivirus/antimalware deberá de ser compatible con cualquier plataforma de virtualización, así como funcionalmente hablando no deberá requerir la instalación de ningún plugin o complemento instalado y evidente desde "Control Panel -> Agregar o Quitar programas".

Protección	Especificación Técnica
	Solución a contratarse deberá provisionar capacidad para generar CD y/o USB Booteables, los cuales posean capacidad de análisis para la inspección de malware en máquinas que no cuenten con la protección de solución contratada o requieran del uso de los mismos con el fin de eliminar cualquier código malicioso, así mismo dichos medios deben poder ser actualizados vía Internet inmediatamente después del arranque desde los mismos.
	Solución a contratarse deberá provisionar capacidad para generar CD y/o USB Booteables, los cuales deberán ofrecer como medio alternativo las siguientes herramientas de diagnóstico y asistencia técnica remota con proveedor o fabricante:
	• Gparted
	• MemTest86+
	• Teamviewer
	• Otras aplicaciones para recibir asistencia remota
	• Otras
	Solución a contratarse deberá cumplir con estándares AMTSO, identificables y validables en cada una de sus pruebas de evidencia técnica; de igual forma fabricante antivirus deberá figurar en el listado de miembros activos de AMTSO.
	Solución a contratarse deberá incluir múltiples capas de seguridad, que deberán operar en forma conjunta y en su defecto tener capacidad de proteger independientemente si alguna de ellas no detecta en un momento dado el vector de ataque; dicho de otra forma, deberá garantizar proteger al ENDPOINT final con diferentes métodos de protección y múltiples capas de seguridad comprobables según documentación de fabricante.
	Incorpore protección a nivel Kernel, previniendo la desactivación y/o alteración por un tercero y/o código malicioso.
	Incorpore auto-protección del núcleo y componentes de la suite de seguridad a nivel ASLR & DEP, así como funcionalmente no requiera de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados “Agregar/Quitar Programas”.
	Incorpore protección en tiempo real contra cualquier alteración al estado del kernel antivirus, imposibilitando detenerlo o dejarlo inoperativo para protección del computador donde ha sido implementado.

Protección	Especificación Técnica
	Integre protección nativa de aprendizaje automático, la cual deberá incluir mecanismos de simulación/detección mediante redes neurales y al menos seis algoritmos de clasificación integrados, dicho módulo de protección deberá coadyuvar en la detección de cualquier tipo de código malicioso nuevo y/o desconocido; así como funcionalmente no debe requerir de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".
	Deberá integrar protección nativa a nivel UEFI que permita comprobar y aplicar seguridad para el entorno previo al inicio y arranque del equipo, dicho modulo deberá detectar componentes maliciosos en el firmware (UEFI/BIOS); funcionalmente no debe requerir de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".
	Incorpore capacidad de protección por contraseña de acceso al propio motor antivirus, a fin de que no pueda ser alterada configuración de la propia solución y/o alteración al estado de protección del computador.
	Instalación de producto podrá realizarse tanto localmente como remotamente desde su consola administrativa; en el término local se entiende se requiere pre compilación de un paquete todo-en-uno para la instalación del producto el cual contenga las pre configuraciones y niveles de seguridad básicos aplicables a la estación de trabajo, así mismo incorpore en un solo paso la unión y sincronización a consola administrativa.
	Comunicación entre clientes administrados (ENDPOINTS) y servidor de administración deberá realizarse mediante conexión SSL cifrada; dicha conexión deberá ser evidente y descrita en el log de estado del agente de conexión mediante cualquier navegador web para fines de validación o auditoria.
	Agente de conexión deberá provisionar log transaccional de referencia, así como en forma simultánea deberá mostrar su estado de conexión y descripción general de sincronizaciones a servidor administrativo; dicho log deberá ser accesible desde cualquier navegador web y en forma dinámica deberá variar en forma automática a fin de evidenciar cualquier problema de comunicación o falla de transferencia y/o comunicación cifrada en la línea del tiempo
	Agente de conexión deberá reportar en forma precisa todo software de terceros y/o fabricante contratado ubicado en el computador que figure como instalado en el equipo donde ha sido instalado.
	Agente de conexión deberá reportar en forma precisa todo hardware instalado en el computador donde ha sido instalado, reportando con precisión todo lo referente al hardware presente.
	Agente de conexión deberá soportar instalación de software de terceros, no delimitando e incluyendo cualquier aplicativo (EXE) que desee ejecutarse o instalarse en los computadores administrados.

Protección	Especificación Técnica
	Solución a contratarse requiere soporte técnico directo del fabricante y que este pueda prestarlo localmente en formato 24x7x365; el mismo en sus modalidades deberá garantizarse ya sea en forma presencial, remota, chat en línea, correo electrónico y/o vía telefónica mediante número local; en caso que la empresa adjudicada por alguna razón no pueda proporcionarlo.
	Nativamente consola de administración deberá poseer soporte para equipos y/o servidores clonados sean estos físicos o virtuales, de forma tal que el identificador por disco o volumen de disco no constituya un problema para identificar individualmente cada equipo administrado.
	Deben incluirse medias de Instalación originales provistas por el fabricante, evidenciables mediante certificado de originalidad provisto por el fabricante y entregado con las mismas.
	Ofertante deberá demostrar experiencia comprobable con respecto al software ofertado para implementación, administración y soporte técnico dentro del territorio nacional que rige este evento para al menos cinco años calendario; en resguardo a los bienes de la institución, así como garantía de cumplimiento del ofertante, no se aceptaran ofertas que no proporcionen la información solicitada y/o bien no presenten las pruebas que así lo demuestren.
	Ofertante deberá demostrar poseer experiencia comprobable para la implementación, administración y soporte técnico en al menos dos clientes que sean igual o superiores a la cantidad total de nodos computacionales que rige este evento; dicho requerimiento será admitido como válido en formalidad únicamente para referencias dentro de territorio nacional, no se aceptaran referencias del extranjero o que no coincidan en su totalidad con el producto ofertado, en resguardo a los bienes de la institución, así como garantía de cumplimiento del ofertante, no se aceptaran ofertas que no proporcionen la información solicitada y/o bien no presenten las pruebas que así lo demuestren
	Ofertante deberá garantizar en totalidad de forma y por escrito que todo tipo de soporte técnico solicitado por esta institución ya sea con el propio ofertante y/o con el fabricante en cualesquiera de sus modalidades 24x7x365 sea totalmente gratuito, así como garantice en su totalidad no aplique ninguna restricción por horas de servicio o similar.
	Ofertante deberá demostrar mediante documento oficial de fabricante, el mismo es un proveedor autorizado para el territorio nacional de sus productos; en caso fabricante no posea oficinas locales dentro del territorio nacional deberá indicarse como no cumplimiento al requerimiento específico sobre dicho aspecto, así como deberá considerarse todo documento que ampare al ofertante como proveedor oficial de solución ofertada cumpla con protocolo de ley para la nacionalización de documentos procedentes del extranjero.

Protección	Especificación Técnica
Host-based Intrusion Prevention System	Incorpore tecnología de control HIPS para estaciones de trabajo y servidores sobre plataforma Microsoft Windows, así como funcionalmente no requiera de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".
	Incorpore HIPS con capacidades avanzadas de protección y funcionalmente sea capaz de realizar las siguientes acciones básicas, pero no limitadas requeridas:
	• Bloquear archivos y/o aplicaciones para ejecución
	• Permitir ejecutar archivos y/o aplicaciones basados en rutas de acceso y/o ficheros en particular
	• Bloquear archivos y/o carpetas contra escritura y/o acceso
	• Permitir escritura y/o acceso para archivos y/o carpetas
	• Bloquear escritura y/o modificación a llaves del registro de sistema
	Incorpore tecnología avanzada que permita prevenir la explotación de vulnerabilidades en las aplicaciones más comunes; principalmente pero no limitado control de explotación para navegadores web, PDF, clientes de correo electrónico, aplicaciones MS Office & Java.
	Incorpore motor de inspección avanzada en memoria operativa que brinde protección contra el malware moderno que ocupa técnicas de cifrado y/o ofuscación.
	Incorpore protección avanzada contra la deshabilitación y/o modificación del propio motor de protección antivirus por parte de terceros y/o algún código malicioso, dicha función deberá reflejarse en el componente HIPS cargado en el sistema.
	Deberá incorporar protección especializada contra ataques del tipo ransomware, la misma deberá ser explícitamente visible dentro del apartado de configuración del producto final adquirido; específicamente el módulo especializado para la prevención del ransomware deberá detectar y bloquear procesos cuyo comportamiento encuadre con la conducta del ransomware en general.
Actualizaciones	Las actualizaciones rutinarias de la base de definición de firmas, deberán de ser pequeñas e incrementales; tanto para actualizaciones rutinarias como para repositorios de distribución (mirror). Se consideran como pequeñas e incrementales a las actualizaciones rutinarias menores a 1MB por cada firma de definición.
	Funcionalmente una actualización rutinaria, debe ser capaz de actualizar firmas antivirus, módulos y/o componentes del sistema antivirus; no incluyendo, pero no limitando la versión de familia del producto contratado y/o futuras versiones del producto adjudicado.

Protección	Especificación Técnica
	Incorpore capacidad para que un cliente instalado (endpoint) pueda convertirse en repositorio de actualizaciones (mirror), con el fin de poder actualizar otros clientes desde este o poder extraer los archivos de actualización y trasladarlos manualmente a otros clientes "stand-alone"; funcionalmente no debe requerir la instalación de módulos adicionales para tales fines, así como no deberá reflejarse como componente adicional en "Agregar/Quitar Programas"
	Deberá poseer factibilidad para actualizar de forma manual todos sus componentes y definiciones de virus, en computadoras sin ningún tipo de conectividad a red; es decir, en status "stand-alone".
	Las actualizaciones de distribución de firmas rutinarias (repositorios de firmas) deberán proveerse a los clientes antivirus internos, mediante servicio HTTP/HTTPS incluido en el propio motor del producto instalado así mismo deberá poder ofrecerse métodos de autenticación básica o vía NTLM a fin de proteger contra el acceso de terceros a firmas antivirus de distribución local; dicha opción deberá integrarse mas no quedar limitada y/o restringida como medio para distribución de firmas mediante motores FTP/Shares de terceros; funcionalmente no debe requerir la instalación de módulos adicionales para tales fines así como no deberá reflejarse como componente adicional en "Agregar/Quitar Programas".
	Las actualizaciones diarias y rutinarias de los componentes del producto se deberán realizar en tiempo real desde Internet o vía LAN Server (Mirror), en forma automática y sin necesidad de intervención del usuario.
	Producto deberá poder actualizar automáticamente desde una unidad extraíble que contenga los ficheros rutinarios de actualización sin intervención alguna del usuario local o bien del personal técnico.
Filtrado de Red y/o Protocolos de Comunicación	Incorpore capacidad de filtrado de protocolos, para todo el tráfico de red; teniendo opción de analizar todo tipo de comunicación saliente/entrante. Funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".
	Incorpore escaneo y limpieza de paquetes en tráfico HTTP, FTP, SMTP y POP3; tanto en los servidores como en las computadoras personales.
	Incorpore filtrado e inspección de protocolos seguros (HTTPS, SMPTS, POP3S, FTPS, entre otros), funcionalmente hablando debe ser capaz de filtrar cualquier comunicación de red segura así como no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".
	Incorpore capacidad de excluir aplicaciones, direcciones IP y/o rangos de direcciones del filtrado de protocolos e inspección al tráfico de red.
	Incorpore capacidad de analizar todo el tráfico de red o bien indicar puertos y/o aplicaciones en particular a inspeccionar a nivel de filtrado de protocolos.

Protección	Especificación Técnica
	Incorpore filtrado básico para listas URL y/o IP de acceso; de tal forma que se pueda controlar efectivamente accesos a los listados estáticos definidos, ya sean sobre comunicación en texto plano (HTTP) o sobre protocolos seguros (HTTPS); funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".
	Incorpore pluguin para el filtrado, análisis y detección antimalware en los clientes de correo electrónico Microsoft Outlook, Windows Mail & Windows Live Mail; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".
	Incorpore tecnología avanzada que integre capas de seguridad previa al host a fin de prevenir la explotación de vulnerabilidades a nivel de red desde host remotos o locales, en forma explícita se requiere proteger el ENDPOINT final contra vulnerabilidades conocidas que puedan afectar a nivel de red aun así no exista parche local instalado en el equipo que desea protegerse Mail; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".
Firewall & IDS	Incorpore firewall/cortafuegos avanzado de doble vía; capaz de filtrar bidireccionalmente el tráfico de red ya sea este entrante o saliente, funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".
	El firewall/cortafuegos incorporado deberá ser totalmente administrable desde cliente o desde consola administrativa, así como deberá poseer modo de solución rápida a problemas comunes guiados intuitivamente desde la propia interfaz del producto.
	Firewall/Cortafuegos incorporado deberá poseer facilidad para la definición de redes de confianza mediante parámetros de detección que faculten identificar si en realidad dispositivo protegido se encuentra en una red "segura" o bien se requiere un modo superior de protección en una red nueva y desconocida.
	Incorpore IDS (Intrusion Detection System) de host para la prevención de acceso no autorizado al computador a nivel de capa de red, funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".
	Incorpore protección anti "BOTNETS", la cual faculte a la solución bloquear el acceso y comunicación a una red botnet así como alertar al usuario de dicha acción y anomalía detectada; funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".

Protección	Especificación Técnica
	Incorpore Control de Vulnerabilidades a nivel de capa de red, el cual deberá inspeccionar y proteger a los protocolos más ampliamente utilizados SMB, RPC y RDP; evitando con dicho fin la propagación del malware, ataques de red dirigidos y la explotación de vulnerabilidades para las que un parche de seguridad aún no está disponible o ha sido desplegado, funcionalmente no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".
Antispam	Incorpore solución antispam a nivel endpoint y posea filtrado para protocolo SMTP, POP3 & IMAP en forma transparente e integrada al producto sin requerir instalación de módulos y/o agentes en el computador; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".
	Incorpore plugin para el filtrado, análisis y clasificación antispam en los clientes de correo electrónico Microsoft Outlook, Windows Mail & Windows Live Mail; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".
	Provea capacidad de generar listas blancas/negras para el filtrado del correo electrónico en la estación de trabajo final y en los clientes de correo electrónico indiciados como compatibles; dicha acción deberá de ser posible realizarse desde el propio producto y/o consola de administración, así como permitirá definir dominios y/o direcciones en cada uno de estos apartados.
Web Filtering	Integre capacidad de Web Filtering basado en categorías, siendo posible definir políticas basadas en grupos de usuario y/o usuarios (tanto a nivel AD como también mediante autenticación local); no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".
	Incorpore capacidad de Web Filtering mediante grupos de categorías, haciendo factible el agrupamiento de múltiples y diferentes categorías de inspección URL para una misma regla de navegación.
	Faculte permitir y/o denegar el acceso URL estáticos mediante reglas configuradas en el Web Filtering.
	Provea posibilidad de agrupamiento en políticas de filtrado URL, siendo factible sumar diferencialmente los accesos y/o denegaciones a fin de aplicar una política final de maquina o grupo de usuarios.

Protección	Especificación Técnica
	Integre capacidad para la generación de logs y sincronización de los mismos a consola corporativa, de acuerdo a cada una de las acciones tomadas en concordancia con la regla URL definida ya sea bloqueo o permisión según sea el caso; dicho log deberá contener toda la información detallada desde el URL bloqueado/permitido hasta el usuario/equipo detectado así como hora/fecha y descripción integra del evento; no debe requerir de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control".
	Integre capacidad Web Filtering sobre sitios URL que ocupen protocolo seguro (HTTPS); no debe requerir de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control".
	Toda regla y/o política para el control URL, deberá poder ser fijada por horarios, días de la semana en particular y/o por usuarios en específico.
Device Control	Incorpore capacidades de "Device Control" administrables ya sea localmente o en forma remota desde su consola administrativa; no debe requerir de instalación y/o módulo reflejado en componentes de programa en "Agregar quitar Programas -> Panel de Control"
	Incorpore capacidades de "Device Control" avanzadas, con el fin de delimitar, denegar o permitir dispositivos portátiles y/o medios extraíbles tales como:
	• Dispositivos de almacenamiento USB
	• Dispositivos ópticos CD/DVD
	• Impresoras USB
	• Dispositivos de almacenamiento Firewire
	• Dispositivos Bluetooth
	• Tarjetas lectoras de memoria
	• Dispositivos de imagen
	• Modems
	• Puertos LPT/COM
	• Dispositivos portátiles (móviles)
	Incorpore funciones avanzadas para el control de dispositivos siendo posible aplicar reglas con el fin de delimitar, denegar o permitir de acuerdo a las siguientes condiciones del dispositivo periférico conectado:

Protección	Especificación Técnica
	• Marca
	• Modelo
	• Serie
	Incorpore funciones avanzadas para el control dispositivos siendo capaz de asignar políticas de acuerdo a grupos de trabajo local o grupos dinámicos mediante un Directorio Activo; así mismo provea extensión de operación por usuario local y/o usuarios de un Directorio Activo.
	Incorpore funciones avanzadas para el control de dispositivos mediante grupos de "dispositivos", siendo posible asignar reglas y/o directrices mediante grupos pre-establecidos de dispositivos con el fin de facilitar administración, así como el control adecuado de los dispositivos conectados a las estaciones de trabajo
	Toda regla y/o política para el control de dispositivos, deberá poder ser fijada por horarios, días de la semana en particular y/o por usuarios en especifico
Endpoint Detection and Response	Incorpore capacidades extendidas para mitigar riesgos extendidos que puedan ser identificados con facilidad mediante una solución específica del tipo Endpoint Detección and Response
	Deberá incorporar sofisticada de detección y respuesta que permita identificar comportamientos anómalos
	Funcionalmente no deberá de depender de alguna consola ubicada en la nube o fuera de las instalaciones de la dependencia, toda funcionalidad requerida es del tipo local, así como deberá permitir en cualquier línea del tiempo inspeccionar, monitorizar o evaluar registros auditables recopilados por la herramienta de Detección y Respuesta solicitada
	Funcionalmente deberá extender las capacidades de detección del endpoint local y al menos permitir detectar y/o responder ante:
	• Detectar las amenazas persistentes avanzadas
	• Detener los ataques sin archivos
	• Bloquear las amenazas 0-day
	• Protegerse del ransomware
	• Neutralizar los ataques patrocinados por el estado
	Funcionalmente deberá ser capaz de indicar con precisión cualquier script ejecutado mediante powershell, dicha funcionalidad deberá proporcionar evidencia total de la línea de comandos ejecutada (strings del script y/o código fuente del mismo)

Protección	Especificación Técnica
	Deberá proporcionar una detección única basada en el comportamiento y en la reputación de archivos, dicha reputación de ficheros deberá estar al día y en constante evaluación mediante telemetría global, misma que deberá permitir en tiempo real evaluar la reputación del fichero, proceso o script analizado
	Deberá permitir configurar la sensibilidad de las reglas de detección para diferentes grupos de computadoras o usuarios, así como permitir eliminar fácilmente las falsas alarmas que pudiese causar alguna regla de detección manual incorporada por el equipo de seguridad de la información
	Deberá permitir combinar criterios como nombre de archivo, ruta, hash, paths, línea de comandos y firmante de aplicación con la finalidad de con precisión las condiciones de activación de las alertas.
	Deberá permitir ubicar con facilidad cualquier comportamiento sospechoso inclusive para eventos pasados, mismo que deberá representarse por cualquier regla de detección nueva agregada.
	Deberá permitir al menos históricos de tres meses consecutivos, mismos que podrán ser evaluados dinámicamente ya sea mediante reglas de detección nuevas o reputación de ficheros obtenidos por indicadores de amenazas de terceros (IOC's) y telemetría global.
	Deberá permitir ubicar cualquier indicador de compromiso de forma tal que permita determinar si una amenaza ya existía antes de la emisión de alerta para alguna regla estática configurada.
	Deberá incluir reglas de detección integradas, así como deberá permitir crear propias reglas para responder a los incidentes detectados
	Funcionalmente deberá permitir bloquear, detener o eliminar cualquier fichero o proceso mediante reglas de acción automatizadas o bien mediante intervención manual de algún operador de seguridad encargado internamente, dicha funcionalidad deberá ser extendida para ejecutar la misma acción sobre todos los computadores en forma simultánea.
	Deberá permitir mayor visibilidad de lo ocurrido en cada computador respecto a ficheros, scripts y/o procesos en general
	Deberá permitir importar o exportar todas sus reglas de detección o acción a formatos XML
	Deberá proporcionar visibilidad total de lo ocurrido, siendo capaz de identificar el origen de una afección en particular, misma visibilidad deberá ser total y no solo representada en una imagen estática, posibilitando de dicha manera descubrir la naturaleza del origen y causa de afección.

SANDBOXING EN LA NUBE-ESET DYNAMIC THREAT DEFENSE.

Protección	Descripción
Cloud Protection	Incorpore tecnología de detección en tiempo real basada en la nube, con el fin de prevenir ataques 0-Day y/o campañas de propagación de malware lanzadas globalmente; dicho alcance deberá garantizarse para correo electrónico, así como todo tipo de tráfico de red, tanto para reputación de archivos, así como vínculos URL.
	Funcionalmente integración de tecnología "Cloud Protection" no deberá requerir de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".
	Incorpore tecnología basada en la nube y en tiempo real, que permita al usuario operador del endpoint verificar la reputación de los procesos activos y de los archivos directamente desde la interfaz del programa o desde el menú contextual.
	Incorpore tecnología sandboxing basada en la nube que integre al menos tres modelos de aprendizaje deep-learning (Deep Machine Learning) así como al menos seis modelos de clasificación para cada modelo Deep Machine Learning aplicado.
	Incorpore capacidad para el envió manual de cualquier tipo de fichero para análisis mediante cloud sandboxing, asi como automáticamente y sin intervención alguna del usuario clasifique, detecte y/o elimine cualquier código malicioso nuevo o desconocido.
	Incorpore tecnología en la nube para la detección de código nuevo y emergente, posibilitando detección del código malicioso y/o vínculo URL inclusive previo al lanzamiento de firmas antivirus de detección estándar.
	Incorpore tecnología "Antiphishing", de tal forma que prevenga al usuario de los intentos de adquirir contraseñas, datos bancarios y/o otra información sensible por parte de los sitios web falsos, haciéndose pasar por los legítimos; funcionalmente no debe requerir la instalación de módulos adicionales para tales fines, así como no deberá reflejarse como componente adicional en "Agregar/Quitar Programas".
	Licenciamiento otorgado deberá poseer garantía y cobertura sobre los sistemas operativos indicados como requeridos, se acepta un solo y único lote de licenciamiento que involucre a todos los sistemas indicados; puntualmente deberá ocuparse una única clave de activación, llave o similar para todos los productos contratados e indicados como compatiblemente requeridos

PROTECTION PARA CORREOS ELECTRONICOS - ESET MAIL SECURITY FOR EXCHANGE ENDPOINT SOLUTIONS G7 EDTD

Protección	Especificación Técnica
	Incluye especificaciones técnicas Generales del PROTECTION PARA ENDPOINTS-ESET ENDPOINT SECURITY, ANTIVIRUS Y ANTISPYWARE.
	Licenciamiento otorgado deberá poseer garantía y cobertura sobre los sistemas operativos indicados como requeridos, se acepta un solo y único lote de licenciamiento que involucre a todos los sistemas indicados; puntualmente deberá ocuparse una única clave de activación, llave o similar para todos los productos contratados e indicados como compatiblemente requeridos
	Licenciamiento adquirido en su totalidad deberá poder ser administrado por una única consola de administración, todos los productos adquiridos para los sistemas operativos indicados como compatibles deberán poderse administrar integralmente desde una única consola validada e implementada en la red interna corporativa
Aspectos Generales	Producto por adquirirse deberá ser totalmente gestionado, así como compatible con consola de administración interna ocupada para el efecto que por nombre se identifica como ESET Security Management Center, formalmente se deberá certificar compatibilidad desde sitio de fabricante donde se corrobore que el producto ofertado sea totalmente compatible con la consola de seguridad ocupada internamente.
	Solución a contratarse requiere soporte técnico directo del fabricante y que este pueda prestarlo localmente en formato 24x7x365; el mismo en sus modalidades deberá garantizarse ya sea en forma presencial, remota, chat en línea, correo electrónico y/o vía telefónica mediante número local; en caso que la empresa adjudicada por alguna razón no pueda proporcionarlo.
	Deben incluirse medias de Instalación originales provistas por el fabricante, evidenciables mediante certificado de originalidad provisto por el fabricante y entregado con las mismas.
	Ofertante deberá demostrar experiencia comprobable con respecto al software ofertado para implementación, administración y soporte técnico dentro del territorio nacional que rige este evento para al menos cinco años calendario; en resguardo a los bienes de la institución, así como garantía de cumplimiento del ofertante, no se aceptaran ofertas que no proporcionen la información solicitada y/o bien no presenten las pruebas que así lo demuestren.

Protección	Especificación Técnica
	Ofertante deberá demostrar poseer experiencia comprobable para la implementación, administración y soporte técnico en al menos dos clientes que sean igual o superiores a la cantidad total de nodos computacionales que rige este evento; dicho requerimiento será admitido como válido en formalidad únicamente para referencias dentro de territorio nacional, no se aceptaran referencias del extranjero o que no coincidan en su totalidad con el producto ofertado, en resguardo a los bienes de la institución, así como garantía de cumplimiento del ofertante, no se aceptaran ofertas que no proporcionen la información solicitada y/o bien no presenten las pruebas que así lo demuestren.
	Ofertante deberá garantizar en totalidad de forma y por escrito que todo tipo de soporte técnico solicitado por esta institución ya sea con el propio ofertante y/o con el fabricante en cualesquiera de sus modalidades 24x7x365 sea totalmente gratuito, así como garantice en su totalidad no aplique ninguna restricción por horas de servicio o similar
	Ofertante deberá demostrar mediante documento oficial de fabricante, el mismo es un proveedor autorizado para el territorio nacional de sus productos; en caso fabricante no posea oficinas locales dentro del territorio nacional deberá indicarse como no cumplimiento al requerimiento específico sobre dicho aspecto, así como deberá considerarse todo documento que ampare al ofertante como proveedor oficial de solución ofertada cumpla con protocolo de ley para la nacionalización de documentos procedentes del extranjero
Antispam	Integre funcionalmente protección para la capa de transporte del correo electrónico provisionado por Servidor Microsoft Exchange en forma totalmente transparente, dicha funcionalidad deberá realizarla tanto para el correo saliente como el correo entrante sin requerir la instalación y/o modulo reflejada en componentes de programa en “Agregar quitar Programas -> Panel de Control”.
	Integre funcionalmente protección Antimalware, Antispam, Anti-Phishing & Análisis mediante cloud sandboxing para todo correo electrónico enviado y/o recibido mediante Servidor Microsoft Exchange; no debe requerir de instalación y/o módulo reflejada en componentes de programa en “Agregar quitar Programas -> Panel de Control”.
	Integre funcionalmente protección antimalware para la base de datos embebida a Microsoft Exchange, de forma tal que pueda protegerse cada buzón de usuario e inclusive realizar análisis retrospectivo para los buzones de correo electrónico que pudiesen haber recibido código malicioso previo a la instalación de dicha solución de seguridad; no debe requerir de instalación y/o módulo reflejada en componentes de programa en “Agregar quitar Programas -> Panel de Control”
	Integre funcionalmente protección antimalware integrada directamente a la base de datos ocupada por Microsoft Exchange, que de forma tal proteja del envió/recepción de código malicioso inclusive cuando se ocupa portal web provisionado por Microsoft Exchange (OWA); no debe requerir de instalación y/o módulo reflejada en componentes de programa en “Agregar quitar Programas -> Panel de Control”

Protección	Especificación Técnica
	Integre funcionalmente protección a nivel de transporte para Microsoft Exchange, de forma tal que al menos pueda realizar lo siguiente:
	• Filtrar correos electrónicos basado en el tipo de documento adjunto (identificador por tipo de ficheros)
	• Filtrar correos electrónicos basado en el contenido del adjunto (identificador de ficheros por tipo y uso)
	• Filtrar correos electrónicos basado en el contenido del cuerpo del mensaje (body message), de forma tal que pueda identificar características, texto o similar contenido en el mismo
	• Filtrar correos electrónicos por tipo de extensión (filtrado de extensiones permitidas)
	• Filtrar correos electrónicos por tamaño del mensaje
	• Filtrar correos electrónicos que hayan sido enviados a múltiples usuarios (cadenas de mensaje)
	• Delimitar cadenas de mensajes o bien identificar y bloquear por medio de contadores cualquier tipo de correo electrónico que encuadre en identificación de cadenas de mensajes (dirigido en forma específica una cantidad de usuarios por definir y totalmente variable, ej: 10, 30, 33 destinatarios en un solo mensaje).
	Incorpore solución antispam a nivel ENDPOINT y posea filtrado para protocolo SMTP, POP3 & IMAP en forma transparente e integrada al producto sin requerir instalación de módulos y/o agentes en el computador; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".
	Incorpore pluguin para el filtrado, análisis y clasificación antispam en los clientes de correo electrónico Microsoft Outlook, Windows Mail & Windows Live Mail; no debe requerir de instalación y/o módulo reflejada en componentes de programa en "Agregar quitar Programas -> Panel de Control".
	Provea capacidad de generar listas blancas/negras para el filtrado del correo electrónico en la estación de trabajo final y en los clientes de correo electrónico indiciados como compatibles; dicha acción deberá de ser posible realizarse desde el propio producto y/o consola de administración, así como permitirá definir dominios y/o direcciones en cada uno de estos apartados.

CONSOLA INTEGRADA PARA LA ADMINISTRACIÓN de ESET-ENDPOINT SECURITY, ESET-DYNAMIC THREAT DEFENSE Y ESET MAIL SECURITY FOR EXCHANGE ENDPOINT SOLUTIONS G7 EDTD

Protección	Especificación Técnica
Generalidades	La consola se debe de integrar con los productos ESET-ENDPOINT SECURITY, ESET-DYNAMIC THREAT DEFENSE Y ESET MAIL SECURITY FOR EXCHANGE ENDPOINT SOLUTIONS
	Servidor de administración y consola administrativa deberá poder implementarse, así como proveer soporte multiplataforma compatible con al menos los siguientes sistemas operativos: Microsoft Windows Server 2019, 2016, 2012R2, 2012, 2008R2 y/o superior
	Microsoft Windows Server Core 2019, 2016, 2012R2, 2012, 2008R2 y/o superior
	Microsoft Windows 11, 10, 8.1, 8 (CAL Microsoft puede limitar el soporte extendido, más sin embargo solución administrativa deberá poder instalarse y ser compatible con sistemas indicados) y/o superior
	RedHat, Debian, Ubuntu, Suse, Fedora & Mandriva así como la mayoría de distribuciones basadas en gestor de paquetes RPM y DEB.
	Servidor de administración y consola administrativa deberá ofrecer compatibilidad para despliegue rápido mediante OVF; a fin de simplificar el despliegue de "Appliance Virtual" para el funcionamiento correcto de servidor administrativo de la solución adquirida.
	Servidor de administración y consola administrativa deberá poder implementarse sobre plataforma Windows mediante un paquete todo en uno que incluya todos los elementos requeridos para instalación simplificada, así como ofrezca un fácil despliegue de solución administrativa; dicho paquete deberá incluir por defecto a los motores de base de datos, así como todo lo que integralmente requiere para su correcto funcionamiento el servidor y consola de administración.
	Servidor de administración y consola administrativa deberá ofrecer compatibilidad con al menos las siguientes bases de datos:
	· MySQL 5.5 o superior
	· MS SQL Server 2008 R2 o superior
	Servidor de administración y consola administrativa deberá ofrecer una consolidada y completa administración de los productos adquiridos, así como en su totalidad indicar el estado, configuraciones y políticas aplicadas de cada uno de los nodos internos ligados a dicha consola de administración.
	Servidor de administración y consola administrativa deberá ofrecer posibilidad de integración con Active Directory, tanto para instalación remota de clientes, así como para autenticación local de administradores y roles de acceso a la misma.

Protección	Especificación Técnica
	Servidor de administración y consola administrativa deberá ofrecer diversos y variados roles de acceso mediante grupos de usuarios con el fin de definir niveles de acceso a administración de los diferentes recursos que dicha consola administrativa ofrezca a los administradores TI internamente.
	Servidor de administración y consola administrativa deberá provisionar acceso web mediante servidor de aplicaciones JAVA.
	Consola de administración deberá operar en su totalidad en modalidad web, así como integralmente deberá estar desarrollada y compilada sobre código JAVA.
	Servidor de administración y consola administrativa deberá ofrecer posibilidad de segmentación para grandes redes mediante nodos de sincronización remota; de tal forma de facilitar la administración y sincronización de los clientes remotos, dichos nodos de sincronización podrán obrar como gestores de firmas, repositorios locales de instaladores, así como receptores de políticas y estados de los clientes locales.
	Consola de administración deberá ser totalmente web, así como funcionalmente deberá ser compatible con cualquier navegador web tanto en sistemas operativos Microsoft, GNU/Linux, Mac OS y/o cualquier otro que a conveniencia pueda ocuparse para el acceso a dicha consola de administración.
	Consola de administración web deberá garantizarse para al menos los siguientes navegadores en las versiones indicadas o superiores, sin requerir la instalación de algún plugin y/o complemento adicional del lado del cliente final: • Firefox 20+ • Internet Explorer 10+ • Chrome 23+ • Safari 6+ • Opera 12+
	Consola de administración web deberá ofrecer por completo administración para todos los productos ofertados independientemente del sistema operativo donde corre cliente o servidor, de forma tal que en su totalidad y absolutamente todos los productos sean administrados desde una sola interfaz web.
	Consola de administración debe incorporar Dashboard accesibles desde cualquier navegador web y desde cualquier punto dentro o fuera de la red local; no debe requerir para dicha operación el uso de IIS o motor diferente al integrado nativamente por la solución.
	Consola de Administración no deberá requerir de la existencia de un Dominio de Autenticación de Usuarios para su buen funcionamiento o como condicionante de operación; sin embargo, deberá permitir administrar clientes antivirus en distintos grupos de trabajo o multi-dominios ya existentes.
	Consola de administración web no deberá requerir para su funcionamiento u operar sobre plataformas ASP, JSP o PHP.

Protección	Especificación Técnica
	Consola de administración deberá manejar múltiples tipos de Licencias de Software, en diferentes cantidades de equipos y fechas de expiración.
	Consola de administración no deberá requerir el uso de MMC (Microsoft Management Console) para el funcionamiento de la misma o como requisito de instalación.
	En términos de una correcta administración se requiere que una configuración establecida para un determinado cliente (ENDPOINT) pueda ser exportada, tanto desde la Consola de Administración, como desde el mismo cliente, para poder ser importada en otros clientes, de ser necesario.
	Consola de administración deberá facultar instalación remota desatendida ya sea ocupando autenticación local o vía un directorio de autenticación, no importando si esta se realiza en dominio o en grupos de trabajo.
	Consola y servidor de administración no deben requerir System Center Configuration Manager (SCCM), CM12, CM0, ConfigMgr, Configuration Manager o similar para uso de consola administrativa y/o servidor de administración; no debe figurar en especificaciones del fabricante (web/datasheets).
	Servidor central de administración (consola/servidor) deberá ser compatible a nivel de almacenamiento de registros (logs) con base de datos MySQL y SQL Server; dicha compatibilidad deberá garantizar funcionamiento correcto con versiones “libre de pago” de dichas bases de datos (MySQL Community Edition & MS SQL Server Express).
	Servidor central de administración deberá proveer compatibilidad con SYSLOG en forma nativa, de tal forma que los eventos ocurridos en los clientes puedan ser interpretados por un syslog server.
	Consola y servidor de administración no deberán requerir Microsoft Message Queue como requisito para instalación y/o operación.
	Consola/Servidor deberá provisionar doble factor de autenticación (2FA) para su interfaz web de administración; nativamente deberá ofertarse al menos en forma gratuita hasta cinco operadores y no deberá requerir de hardware/software que requiera pago o licenciamiento adicional.
	Producto por adquirirse deberá funcionalmente ser compatible con consola de administración ESET Security Management Center ofreciendo integración para al menos las siguientes herramientas de centralización: • CconnectWise Automate • Datto RMM • SolarWinds • Ninja RMM

Protección	Especificación Técnica
	Consola de administración deberá funcionalmente ofrecer protección contra ataques de fuerza bruta, inactivando acceso a la fuente origen (IP) que ha causado afección y/o bien habilitando funcionalidades extendidas de seguridad por medio de un doble factor de autenticación.
	Debe ser compatible con la solución actual
	Producto por adquirirse deberá ser totalmente gestionado, así como compatible con consola de administración interna ocupada para el efecto que por nombre se identifica como ESET Security Management Center, formalmente se deberá certificar compatibilidad desde sitio de fabricante donde se corrobore que el producto ofertado sea totalmente compatible con la consola de seguridad ocupada internamente
	Incorpore protección en tiempo real contra todo tipo de malware; incluyendo virus, gusanos, troyanos, spyware, phishing, rootkit, adware, riskware, keyloggers y/o otros códigos maliciosos nuevos y desconocidos. Específicamente para dicho fin no deberá depender de que el Sistema Operativo del "Endpoint/Cliente" tenga las actualizaciones y Service Pack al día
	Incorpore protección contra virus boot, virus macros, virus residentes en RAM, virus de acción directa, virus encriptados, virus polimórficos, virus de FAT, etc
	Deberá integrar sandbox incorporado en el propio producto, con el objetivo de contener amenazas, emularlas, detectarlas y eliminarlas; dicha protección en particular deberá ser capaz de observar el comportamiento en tiempo real de cualquier binario en memoria operativa (RAM), siendo capaz de detectar basado en patrones de comportamiento & ML amenazas nuevas y desconocidas del tipo 0Day, APT's y/o cualquier tipo de código malicioso emergente
	Incorpore motor heurístico proactivo y preciso de tecnología avanzada, dicho motor debe ser propio y no de terceros fabricantes y/o colaboraciones externas ajenas a casa matriz
	Incorpore detección de virus en archivos compactados, sin importar el número de niveles de compresión, en los formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y/o otros
	Integralmente hablando producto instalado en el computador no deberá presentar fragmentación para su correcto funcionamiento (múltiples módulos instalados en el computador reflejados en programas instalados "Agregar/Quitar Programas" no serán aceptados, exceptuando únicamente al agente de conexión)
	Deberá permitir importar o exportar configuraciones de clientes de manera fácil, vía archivos xml livianos y transportables.
	Incorpore capacidad de poder enviar a los centros de soporte técnico las muestras de virus o códigos maliciosos, con la finalidad de que puedan ser analizados, y clasificados para su contingencia inmediata directamente desde la interfaz gráfica

Protección	Especificación Técnica
	Incorpore capacidad de generar casos de soporte vía la interfaz gráfica de la solución.
	Incorpore chequeo y control de Actualizaciones para Microsoft Windows, dicho control debe ser capaz de ser configurado para reportar diferentes niveles de actualización o desactivar el informe de las mismas.
	Toda configuración a nivel de clientes, deberá poder ser posible realizarse desde consola administrativa y funcionalmente podrá gestionarse integralmente desde una única consola administrativa centralizada. Queda implícitamente descrito todos los productos adquiridos deberán administrarse desde una sola consola de administración, no importando el sistema operativo sobre el cual hayan sido implementados.
	Incorpore compatibilidad nativa en su interfaz gráfica con dispositivos que integren tecnología TouchScreen
	Incorpore cache local de inspección a fin de mejorar el rendimiento en equipos virtualizados, explícitamente la cache de inspección local deberá validar si los ficheros fueron inspeccionados previamente por otro equipo en la red y en todo caso no forzar inspección local si el mismo es sano e inocuo al sistema a fin de acelerar el proceso de inspección. Dicha cache en aceleración de inspección antivirus/antimalware deberá de ser compatible con cualquier plataforma de virtualización, así como funcionalmente hablando no deberá requerir la instalación de ningún pluguin o complemento instalado y evidente desde "Control Panel -> Agregar o Quitar programas"
	Solución a contratarse deberá provisionar capacidad para generar CD y/o USB Booteables, los cuales posean capacidad de análisis para la inspección de malware en máquinas que no cuenten con la protección de solución contratada o requieran del uso de los mismos con el fin de eliminar cualquier código malicioso, así mismo dichos medios deben poder ser actualizados vía Internet inmediatamente después del arranque desde los mismos.
	Solución a contratarse deberá provisionar capacidad para generar CD y/o USB Booteables, los cuales deberán ofrecer como medio alternativo las siguientes herramientas de diagnóstico y asistencia técnica remota con proveedor o fabricante: - Gparted - MemTest86+ - Teamviewer - Otras aplicaciones para recibir asistencia remota - Otras
	Solución a contratarse deberá cumplir con estándares AMTSO, identificables y validables en cada una de sus pruebas de evidencia técnica; de igual forma fabricante antivirus deberá figurar en el listado de miembros activos de AMTSO

Protección	Especificación Técnica
	Solución a contratarse deberá incluir múltiples capas de seguridad, que deberán operar en forma conjunta y en su defecto tener capacidad de proteger independientemente si alguna de ellas no detecta en un momento dado el vector de ataque; dicho de otra forma, deberá garantizar proteger al endpoint final con diferentes métodos de protección y múltiples capas de seguridad comprobables según documentación de fabricante.
	Incorpore protección a nivel Kernel, previniendo la desactivación y/o alteración por un tercero y/o código malicioso.
	Incorpore auto-protección del núcleo y componentes de la suite de seguridad a nivel ASLR & DEP, así como funcionalmente no requiera de instalación de modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".
	Incorpore protección en tiempo real contra cualquier alteración al estado del kernel antivirus, imposibilitando detenerlo o dejarlo inoperativo para protección del computador donde ha sido implementado.
	Integre protección nativa de aprendizaje automático, la cual deberá incluir mecanismos de simulación/detección mediante redes neurales y al menos seis algoritmos de clasificación integrados, dicho módulo de protección deberá coadyuvar en la detección de cualquier tipo de código malicioso nuevo y/o desconocido; así como funcionalmente no debe requerir de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas".
	Deberá integrar protección nativa a nivel UEFI que permita comprobar y aplicar seguridad para el entorno previo al inicio y arranque del equipo, dicho modulo deberá detectar componentes maliciosos en el firmware (UEFI/BIOS); funcionalmente no debe requerir de la instalación de cualquier modulo y/o componente de sistema adicional reflejado en programas instalados "Agregar/Quitar Programas"
	Incorpore capacidad de protección por contraseña de acceso al propio motor antivirus, a fin de que no pueda ser alterada configuración de la propia solución y/o alteración al estado de protección del computador.
	Instalación de producto podrá realizarse tanto localmente como remotamente desde su consola administrativa; en el término local se entiende se requiere pre compilación de un paquete todo-en-uno para la instalación del producto el cual contenga las pre configuraciones y niveles de seguridad básicos aplicables a la estación de trabajo, así mismo incorpore en un solo paso la unión y sincronización a consola administrativa.
	Comunicación entre clientes administrados (endpoints) y servidor de administración deberá realizarse mediante conexión SSL cifrada; dicha conexión deberá ser evidente y descrita en el log de estado del agente de conexión mediante cualquier navegador web para fines de validación o auditoria.

Protección	Especificación Técnica
	Agente de conexión deberá provisionar log transaccional de referencia, así como en forma simultánea deberá mostrar su estado de conexión y descripción general de sincronizaciones a servidor administrativo; dicho log deberá ser accesible desde cualquier navegador web y en forma dinámica deberá variar en forma automática a fin de evidenciar cualquier problema de comunicación o falla de transferencia y/o comunicación cifrada en la línea del tiempo.
	Agente de conexión deberá reportar en forma precisa todo software de terceros y/o fabricante contratado ubicado en el computador que figure como instalado en el equipo donde ha sido instalado.
	Agente de conexión deberá reportar en forma precisa todo hardware instalado en el computador donde ha sido instalado, reportando con precisión todo lo referente al hardware presente.
	Agente de conexión deberá soportar instalación de software de terceros, no delimitando e incluyendo cualquier aplicativo (EXE) que desee ejecutarse o instalarse en los computadores administrados.
	Solución a contratarse requiere soporte técnico directo del fabricante y que este pueda prestarlo localmente en formato 24x7x365; el mismo en sus modalidades deberá garantizarse ya sea en forma presencial, remota, chat en línea, correo electrónico y/o vía telefónica mediante número local; en caso que la empresa adjudicada por alguna razón no pueda proporcionarlo.
	Nativamente consola de administración deberá poseer soporte para equipos y/o servidores clonados sean estos físicos o virtuales, de forma tal que el identificador por disco o volumen de disco no constituya un problema para identificar individualmente cada equipo administrado
	Deben incluirse medias de Instalación originales provistas por el fabricante, evidenciables mediante certificado de originalidad provisto por el fabricante y entregado con las mismas.
	Ofertante deberá demostrar experiencia comprobable con respecto al software ofertado para implementación, administración y soporte técnico dentro del territorio nacional que rige este evento para al menos cinco años calendario; en resguardo a los bienes de la institución, así como garantía de cumplimiento del ofertante, no se aceptaran ofertas que no proporcionen la información solicitada y/o bien no presenten las pruebas que así lo demuestren.
	Ofertante deberá demostrar poseer experiencia comprobable para la implementación, administración y soporte técnico en al menos dos clientes que sean igual o superiores a la cantidad total de nodos computacionales que rige este evento; dicho requerimiento será admitido como válido en formalidad únicamente para referencias dentro de territorio nacional, no se aceptaran referencias del extranjero o que no coincidan en su totalidad con el producto ofertado, en resguardo a los bienes de la institución, así como garantía de cumplimiento del ofertante, no se aceptaran ofertas que no proporcionen la información solicitada y/o bien no presenten las pruebas que así lo demuestren.

Protección	Especificación Técnica
	Ofertante deberá garantizar en totalidad de forma y por escrito que todo tipo de soporte técnico solicitado por esta institución ya sea con el propio ofertante y/o con el fabricante en cualesquiera de sus modalidades 24x7x365 sea totalmente gratuito, así como garantice en su totalidad no aplique ninguna restricción por horas de servicio o similar.
	Ofertante deberá demostrar mediante documento oficial de fabricante, el mismo es un proveedor autorizado para el territorio nacional de sus productos; en caso fabricante no posea oficinas locales dentro del territorio nacional deberá indicarse como no cumplimiento al requerimiento específico sobre dicho aspecto, así como deberá considerarse todo documento que ampare al ofertante como proveedor oficial de solución ofertada cumpla con protocolo de ley para la nacionalización de documentos procedentes del extranjero.

SECCION IV – FORMULARIOS Y FORMATOS

Índice de Formularios y Formatos

LISTA DE PRECIOS

País del Comprador Honduras				Monedas de conformidad con la Sub cláusula 09.4 del IO-09			Fecha: _____ LPN No: _____ Alternativa No: _____ Página No. _____	
1	2	3	4	5	6	7	8	9
No. de Artículo	Descripción de los Bienes	Fecha de entrega	Cantidad y unidad física	Precio Unitario entregado en [indicar lugar de destino convenido] de cada artículo	Precio Total por cada artículo (Col. 4´5)	Lugar del Destino Final	Impuestos sobre la venta otros pagaderos por artículo	Precio Total por artículo (Col. 6+8)
[indicar No. de artículo]	*[indicar nombre de los bienes]*	*[indicar la fecha de entrega ofertada]*	*[indicar el número de unidades a proveer y el nombre de la unidad física de medida]*	*[indicar precio unitario]*	*[indicar precio total por cada artículo]*	*Indicar el lugar de destino convenido, según la CC-04 Lugar de Entrega del Suministro*	*[indicar impuestos sobre la venta y otros pagaderos por artículo si el contrato es adjudicado]*	*[indicar precio total por artículo]*
							Precio Total	

Observación; **Presentar la oferta económica según cuadro indicado en fase 5 evaluación económica.** Formulario de Información sobre el Oferente.

FORMULARIO DE INFORMACIÓN SOBRE EL OFERENTE

[El Oferente deberá completar este formulario de acuerdo con las instrucciones siguientes. No se aceptará ninguna alteración a este formulario ni se aceptarán substitutos.]

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

Página de páginas

1. Nombre jurídico del Oferente *[indicar el nombre jurídico del Oferente]*
2. Si se trata de un Consorcio, nombre jurídico de cada miembro: *[indicar el nombre jurídico de cada miembro del Consorcio]*
3. País donde está constituido o incorporado el Oferente en la actualidad o País donde intenta constituirse o incorporarse *[indicar el país de ciudadanía del Oferente en la actualidad o país donde intenta constituirse o incorporarse]*
4. Año de constitución o incorporación del Oferente: *[indicar el año de constitución o incorporación del Oferente]*
5. Dirección jurídica del Oferente en el país donde está constituido o incorporado: [*indicar la Dirección jurídica del Oferente en el país donde está constituido o incorporado]*
6. Información del Representante autorizado del Oferente:

   Nombre: *[indicar el nombre del representante autorizado]*

   Dirección: *[indicar la dirección del representante autorizado]*

   Números de teléfono y facsímile*: [indicar los números de teléfono y facsímile del representante autorizado]*

   Dirección de correo electrónico: *[indicar la dirección de correo electrónico del representante autorizado]*

7. Se adjuntan copias de los documentos originales de: *[marcar la(s) casilla(s) de los documentos originales adjuntos]*

- Estatutos de la Sociedad de la empresa de conformidadcon las Sub cláusulas 09.1 de la IO-09.
- Si se trata de un Consorcio, carta de intención de formar el Consorcio, o el Convenio de Consorcio, de conformidad con la cláusula 5.1 de la IO-05.
- Si se trata de un ente gubernamental Hondureño, documentación que acredite su autonomía jurídica y financiera y el cumplimiento con las leyes comerciales, de conformidad con la Sub cláusula 09.1, 09.2, 09.03 y 09.4 de la IO-09.

FORMULARIO DE INFORMACIÓN SOBRE LOS MIEMBROS DEL CONSORCIO

[El Oferente y cada uno de sus miembros deberán completar este formulario de acuerdo con las instrucciones indicadas a continuación]

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

Página ____ de ____ páginas

1. Nombre jurídico del Oferente *[indicar el nombre jurídico del Oferente]*
2. Nombre jurídico del miembro del Consorcio *[indicar el Nombre jurídico del miembro del Consorcio]*
3. Nombre del País de constitución o incorporación del miembro del Consorcio *[indicar el nombre del País de constitución o incorporación del miembro del Consorcio]*
4. Año de constitución o incorporación del miembro del Consorcio: *[indicar el año de constitución o incorporación del miembro del Consorcio]*
5. Dirección jurídica del miembro del Consorcio en el País donde está constituido o incorporado: *[Dirección jurídica del miembro del Consorcio en el país donde está constituido o incorporado]*
6. Información sobre el Representante Autorizado del miembro del Consorcio: Nombre: *[indicar el nombre del representante autorizado del miembro del Consorcio]* Dirección: *[indicar la dirección del representante autorizado del miembro del Consorcio]* Números de teléfono y facsímile*: [[indicar los números de teléfono y facsímile del representante autorizado del miembro del Consorcio]* Dirección de correo electrónico: *[[indicar la dirección de correo electrónico del representante autorizado del miembro del Consorcio]*

7. Copias adjuntas de documentos originales de: *[marcar la(s) casillas(s) de los documentos adjuntos]*

☐ Estatutos de la Sociedad de la empresa de conformidadcon las Sub cláusulas 09.1 de la IO-09.

☐ Si se trata de un ente gubernamental Hondureño, documentación que acredite su autonomía jurídica y financiera y el cumplimiento con las leyes comerciales, de conformidad con la Sub cláusula 09.1, 09.2, 09.03 y 09.4 de la IO-09.

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: *[**según invitación a licitar**) de la presentación de la Oferta]*

LPN No.*: [**14-2022**]*

Llamado a Licitación No.: *[**14-2022**]*

Alternativa No. *[**No se aceptan ofertas alternativas ni parciales, los oferentes presentaran una sola oferta**]*

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];*

N°	CONCEPTO	CANTIDAD	UNIDAD	PRECIO UNITARIO	PRECIO TOTAL
1					
2					
				OFERTA TOTAL	

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

El valor de la oferta deberá comprender todos los impuestos correspondientes.

(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 cláusula IO-06, a partir de la fecha límite fijada para la presentación de las ofertas de conformidad con la cláusula IO-05. 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 Cumplimientodel Contrato de conformidad con la Cláusula CC-07 de las condiciones de contratación;

(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) 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”.)

(i) 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.

(j) 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 EstadoCivil _____, de Nacionalidad_____, con domicilio en _____,

Y con Documento Nacional de Identificación/Pasaporte No_____, actuando en mi condición de Representante Legal de *(indicar el nombre de la empresa oferente/ En caso de Consorcio indicar el nombre de las empresas que lo integran)*, por la presente HAGO DECLARACION JURADA: Que ni mi persona ni mi representada se encuentran comprendido en ninguna de la prohibiciones o inhabilidades a que se refiere los artículos 15 y 16 de la Ley de Contratación del Estado.

En fe de lo cual firmo la presente en la ciudad de_____, Municipio de_____, Departamento de_____, a los____días del mes_____del año_____.

Firma y Sello_____

(en caso de persona Natural solo Firma)

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

DECLARACIÓN JURADA DE NO ESTAR COMPRENDIDO EN LOS ARTICULOS 36, 37, 38, 39, 40 Y 41 DE LA LEY ESPECIAL CONTRA EL LAVADO DE ACTIVOS

DECLARACIÓN JURADA DE NO ESTAR COMPRENDIDO EN LOS ARTICULOS 36, 37, 38, 39, 40 Y 41 DE LA LEY ESPECIAL CONTRA EL LAVADO DE ACTIVOS

Yo, _____ (descripción de las generales) en mi condición personal y de mí representada la empresa _____ (nombre de la compañía), para efectos de participar en el Proceso de LICITACIÓN PÚBLICA NACIONAL Nº: _____ responsablemente DECLARO Y JURO que no nos encontramos comprendidos en lo dispuesto en los *artículos 36, 37, 38, 39, 40 y 41 de la Ley Especial Contra Lavado de Activos* los cuales disponen:

Artículo 36.- Incurre en el delito de lavado de activos: quien por sí o por interpósita persona: Adquiera invierta, transforme, resguarde, administre, custodie, transporte, transfiera, convierta, conserve, traslade, oculte, encubra, de apariencia de ilegalidad, legalice o impida la determinación del origen o la verdadera naturaleza, así como la ubicación, el destino el movimiento o la propiedad de activos productos directos o indirectos de las actividades de tráfico ilícito de drogas, trata de personas, tráfico ilegal de armas, falsificación de moneda, tráfico de órganos humanos, hurto o robo de vehículos automotores, robo a instituciones financieras, estafas o fraudes financieros en las actividades de la administración del Estado a empresas privadas o particulares, secuestro, extorsión, financiamiento de terrorismo, terrorismo, tráfico de influencias y delitos conexos y cualesquiera otro que atenten contra la Administración Privada, la Libertad y seguridad, de los recursos naturales y el medio ambiente; o que no tengan causa o justificación económica o licita de su procedencia.

Artículo 37.- Quien preste su nombre en actos o contratos reales o simulados, de carácter civil o mercantil, que se refieran a la adquisición, transferencias o administración de bienes que: procedan directa o indirectamente de las actividades de tráfico ilícito de drogas, trata de personas, tráfico ilegal de armas, falsificación de moneda, tráfico de órganos humanos, hurto o robo de vehículos automotores, robo a instituciones financieras, estafas o fraudes financieros en las actividades de la Administración del Estado, privadas o particulares, secuestro, extorsión, financiamiento del terrorismo, terrorismo, tráfico de influencias y delitos conexos y cualesquiera otro que atenten contra la Administración Pública, la libertad y seguridad, los recursos naturales y el medio ambiente; o que no tengan causa o justificación económica o lícita de su procedencia.

Artículo 38.- Quienes se asocien o confabulen para cometer el delito de lavado de activos o testaferrato deben ser sancionados por ese solo hecho, con reclusión de seis (6) a diez (10) años.

Artículo 39.- Autor del delito de encubrimiento de lavado de activos, se le debe sancionar con la pena señalada en el Artículo 38 de esta Ley rebajada en un tercio (1/3).

Artículo 40.- El Empleado o Funcionario Público que valiéndose de su cargo participe, facilite o se beneficie en el desarrollo de delitos de lavado de activos, encubrimiento del delito de lavado de activos o en la asociación para la ejecución de lavado de activos, debe ser sancionado con una pena igual a la establecida en el Artículo 38 de esta Ley, aumentada en un cuarto (1/4) y la inhabilitación absoluta definitiva en el ejercicio de cualquier cargo público, como penas principales.

La pena indicada en este Artículo también se debe aplicar los representantes legales de las personas jurídicas que hayan participado en la comisión de este delito.

Artículo 41. El Sujeto Obligado que por la omisión en cumplimiento de las obligaciones de la Debida Diligencia y prevención de lavado de activos facilitare la realización de esta conducta, se le debe sancionar con reclusión de dos (2) a cinco (5) años, a menos que la conducta desplegada se encuentre sancionada con una pena mayor.

Para constancia se firma la presente Declaración Jurada responsablemente, en la ciudad de _____ a los____ días del mes de _____del año _____.

FIRMA Y SELLO

DECLARACIÓN JURADA DE LA ENTIDAD GARANTE

Yo, _____ en mi condición de _____

Declaro y juro en forma responsable y para efectos de cumplimiento de los Artículos 241 y 242 del Reglamento de la Ley de Contratación del Estado que:

1. Mi representada no se encuentra en mora frente a la administración, incluyendo cualquier organismo del sector público, como consecuencia de la falta de pago de garantías ejecutadas;

2. Mi representada no se encuentra en situación de suspensión de pagos o de liquidación forzosa;

3. Mi representada no se encuentra suspendida la autorización administrativa para el ejercicio de su actividad;

4. Mi representada se obliga en forma solidaria con el garantizado, con renuncia expresa al beneficio de excusión."

De igual forma declaro que la firma que aparece suscribiendo la Garantía _____es de funcionarios de esta institución_____ con poder suficiente para obligar al _____.

Para constancia se firma la presente Declaración Jurada responsablemente, en la ciudad de _____ a los _____días del mes de _____ del año _____.

Firma y sello

FORMULARIO DECLARACIÓN JURADA DE INTEGRIDAD

YO_____, Mayor de edad, de Estado Civil _____, de Nacionalidad_____, con domicilio en _____,

Y con Documento Nacional de Identificación (DNI)/Pasaporte No_____, actuando en mi condición de Representante Legal de_____, por la presente **HAGO DECLARACION JURADA DE INTEGRIDAD**: Que mi persona y mi representada se comprometen a:

1.- A practicar las más elevadas normas éticas durante el presente proceso de contratación.

2.- Abstenernos de adoptar conductas orientas a que los funcionarios o empleados involucrados en el presente proceso de contratación induzcan a alterar el resultado del proceso u otros aspectos que pudieran otorgar condiciones más ventajosas en relación a los demás participantes.

3.- A no formular acuerdos con otros proveedores participantes o a la ejecución de acciones que sean constitutivas de:

PRACTICA CORRUPTA: Que consiste en ofrecer, dar, recibir, o solicitar, directa o indirectamente, cualquier cosa de valor para influenciar indebidamente las acciones de otra parte.

PRACTICA DE FRAUDE: Que es cualquier acto u omisión, incluida la tergiversación de hechos y circunstancias, que deliberada o imprudentemente engañen, o intenten engañar, a alguna parte para obtener un beneficio financiero o de otra naturaleza o para evadir una obligación.

PRACTICA DE COERCION: Que consiste en perjudicar o causar daño, o amenazar con perjudicar o causar daño, directa o indirectamente, a cualquier parte o a sus bienes para influenciar indebidamente las acciones de una parte.

PRACTICA DE COLUSION: Que es un acuerdo entre dos o más partes realizado con la intención de alcanzar un propósito inapropiado, lo que incluye influenciar en forma inapropiada las acciones de otra parte.

PRACTICA DE OBSTRUCCION: Que consiste en a) destruir, falsificar, alterar u ocultar deliberadamente evidencia significativa para la investigación o realizar declaraciones falsas ante los investigadores con el fin de impedir materialmente una investigación sobre denuncias de una práctica corrupta, fraudulenta, cohersiva o colusoria; y/o amenazar, hostigar o intimidar a cualquier parte para impedir que divulgue su conocimiento de asuntos que son importantes para la investigación o que prosiga la investigación, o b) todo acto dirigido a impedir materialmente el ejercicio de los derechos del Estado.

4.- Así mismo declaro que entiendo que las acciones antes mencionadas son ilustrativas y no limitativas de cualquier otra acción constitutiva de delito o contraria al derecho en perjuicio del patrimonio del Estado de Honduras; por lo que expreso mi sumisión a la legislación nacional vigente.

5.- Declaro que me obligo a regir mis relaciones comerciales con las Instituciones de Estado de Honduras bajos los principios de la buena fe, la transparencia y la competencia leal cuando participen en procesos de licitaciones, contrataciones, concesiones, ventas, subastas de obras o concursos.

6.- Declaro que mi representada no se encuentra en ninguna lista negra o en la denominada lista Clinton (o cualquier otra que la reemplace, modifique o complemente), en la lista Engel, ni que haber sido agregado enla lista OFAC (Oficina de Control de Activos Extranjeros del Tesoro del EEUU), así como que ninguno de sus socios, accionistas o representantes legales se encuentren impedidos para celebrar actos y contratos que violenten la Ley Penal.

7.- Autorizo a la institución contratante para que realice cualquier investigación minuciosa en el marco del respeto y al debido proceso sobre prácticas corruptivas en las cuales mi representada haya o este participando. Promoviendo de esa manera practicas éticas y de buena gobernanza en los procesos de contratación.

En fe de lo cual firmo la presenta en la ciudad_____municipio de _____, Departamento de_____a los_____, días del mes de_____del año_____.

FIRMA Y SELLO

(en caso de persona Natural solo Firma)

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

CONTRATO

CONTRATO No.---------- DEL PROCESO DE LA LICITACION PÚBLICA NACIONAL No.-14-2022 "RENOVACIÓN LICENCIAMIENTO DE SOFTWARE ANTIVIRUS PARA EL PODER JUDICIAL.

Este Contrato se celebra **en la ciudad de Tegucigalpa, M.D.C** .el día_____ del mes de_____ del año_____ entre **ROLANDO EDGARDO ARGUETA PÉREZ** mayor de edad, hondureño, casado, Abogado y Notario de este domicilio, con Documento Nacional de Identificación número 1313-1972-00117, actuando en mi condición de Presidente de la Corte Suprema de Justicia, según Decreto Legislativo número 09-2016 publicado en el Diario Oficial La Gaceta bajo número 33962 de fecha 17 de febrero del 2016 y debidamente facultado para organizar y dirigir administrativamente al Poder Judicial según artículo 3 transitorio del Decreto Número 5-2011 para la celebración de este contrato , en adelante denominado **EL PODER JUDICIAL (CONTRATANTE)** y (nombre completo)____ **_____,** mayor de edad, casado, Ingeniero …….., y de este domicilio y con documento nacional de identificación No. _____, actuando en su condición de Representante Legal de la Empresa, _____ con RTN _____, constituida el –------ de---------- de ----------, según Instrumento Público ------,---- autorizado por el Notario ---------- con número de Exequatur ---------- e inscrito bajo el Número -----, del folio----- y ----- tomo -----, del Registro de Comerciantes Sociales de ---------- Departamento de --------, en adelante denominado **EL PROVEEDOR** por la otra parte.- Por cuanto **EL PODER JUDICIAL** (CONTRATANTE) desea que el **PROVEEDOR** realice la entrega del suministro indicado en la Licitación P…. Nacional No._____ en adelante denominado "el suministro" y EL PODER JUDICIAL (CONTRATANTE) ha aceptado la Oferta para la entrega del suministro hasta su finalización así como la subsanación de cualquier defecto del mismo. En observancia al Pliego de Condiciones, Ley de Contratación del Estado y su Reglamento, en consecuencia, este Contrato atestigua lo siguiente: **CLAUSULA PRIMERA:** En este Contrato las palabras y expresiones tendrán el mismo significado que respectivamente se les ha asignado en los documentos utilizados en el proceso de contratación, a los que se hace referencia en adelante y los mismos se considerarán parte de este Contrato y se

leerán e interpretarán como parte del mismo. **CLAUSULA SEGUNDA: ANTECEDENTES.- 1)** Mediante Oficio No. -----DAPJ------ de fecha……de……de. 202----- la Dirección Administrativa solicitó autorización para dar inicio al Proceso de Contratación para el "suministro de…(describir los materiales o equipo, etc..), **2)** Mediante Memorando PCSJ----------, de fecha ----- de enero de -----, se solicitó disponibilidad presupuestaria a la Dirección de Planificación, Presupuesto y Financiamiento; **3)** Según oficio DPPF-DCYM--------, de fecha --- de --------- de ----, suscrito por la Directora de Planificación, Presupuesto y Financiamiento, confirmó la disponibilidad presupuestaria; **4)** Mediante memorando PCSJ N° -------- y auto de fecha --- de ----- de ------, la Presidencia del Poder Judicial autorizó el inicio del proceso de contratación para adquirir el suministro de…….**5)** Mediante Dictamen Legal, por parte de la Dirección de Asesoría Jurídica, de fecha ---- de ------- de 2-------, concluyó que el documento base está en apego a las disposiciones legales vigentes en la materia; **6)** Mediante Oficio No.----ULPJ-202--- de fecha ---de-----de---- 202--- EL Jefe de la Unidad de Licitaciones, solicitó al Comprador Público Certificado No.100 la Certificación de Calidad de la documentación del proceso de Licitación P…Nacional No.----- del presente suministro; **7)** Mediante Oficio No.---202---CPC-PJ de fecha --- de ----de----202---suscrito por el Comprador Público Certificado No.0100 contentivo del Visto Bueno B-----202---Certifica que la documentación se ajusta al marco regulatorio y normativo pertinente a la Contratación pública. **8)** Mediante Oficio No.---ULPJ-202—de fecha ---de ----de 202---- EL Jefe de la Unidad de Licitaciones solicitó a Presidencia la Aprobación del Documento Base. **9)** Mediante auto emitido por la Presidencia, de fecha --- de ------- de 20----- se aprobó el documento base de la Licitación P……para el "Suministro de -- ----------"; **10)** La invitación a Licitar se publicó, tal y como se establece en el Artículo 46 de la Ley de Contratación del Estado y Artículos 106,107 y 159 de su Reglamento, en los Diarios de mayor circulación y en el Diario Oficial La Gaceta, así : en fecha ------- de --- --de 20------ en el Diario ------- el ----- de_____ de 202----- en el Diario ------, y el día ---- de ----- de 20------, en el Diario Oficial La Gaceta bajo el N° ------- ; **11)** La recepción y apertura de las ofertas del proceso se realizó el----- de ----- de 20----, a las 9:00 a.m., en el Salón de Sesiones de la Dirección de Planificación, Presupuesto y Financiamiento del Poder Judicial; **12)** Mediante auto de la Presidencia, de fecha ---de ----- de 20-----, se designó la Comisión de Evaluación y Análisis y Recomendación de este proceso integrada

por: Abogada_____ en representación de la Presidencia, Abog. ----------por la Unidad de Licitaciones, Abog.. _____por la Dirección de Asesoría Legal, Licenciado(a) _____por la Dirección Administrativa , Ingeniero ._____por el Departamento de Infotecnología y Licenciado(a) _____por Auditoría Interna en calidad de observador **13)** En fecha ------ de ------- de 20----, la Comisión de Evaluación emitió el informe de Revisión, Análisis y Recomendación del proceso; **14)** Mediante Dictamen favorable del informe final, de fecha ---- de ---- de 20----, emitido por Asesoría Legal, es de la opinión que la recomendación hecha por la Comisión de Evaluación y análisis de las ofertas, de adjudicar esta Licitación a la empresa ----------, por un monto de --------- ----------**, (L**----------**)**; es procedente; **15)** Mediante Acuerdo N° PCSJ---20-----, de fecha - de ----- de 20---- y en atención a las consideraciones realizadas por la comisión Evaluadora en su informe final, se acuerda adjudicar el presente proceso de Suministro de…….. a la empresa_____ quien ha cumplido con todos los requerimientos contenidos en los Términos de Referencia, Ley de Contratación del Estado y su Reglamento, se compromete a prestar el servicio de suministro de…… conforme a las entregas presentadas en su oferta y por un monto de ---------- **LEMPIRAS EXACTOS, (L.**----------**)** incluído el 15% del Impuesto sobre venta. **CLAUSULA TERCERA : JUSTIFICACIÓN:……(** según la necesidad que se trate**)……..** de la Licitación P…. No.-_____ para el suministro de ……,…,……,…….según lo estipulado en el Pliego de Condiciones.- **CLÁUSULA CUARTA: OBJETO DEL CONTRATO.-** El suministro consiste en lo siguiente **(**ya sea artículos, bienes, equipos o servicios de…….). **CLÁUSULA QUINTA: ASIGNACIÓN PRESUPUESTARIA:** para la correcta ejecución del presente contrato existe una disponibilidad presupuestaria aprobada de conformidad al Oficio DPPF No…./…22 de fecha _____ de_____ de 202---- emitida por la Dirección de Planificación y Presupuesto del Poder Judicial.- **CLAUSULA SEXTA**: **PRECIO DEL SUMINISTRO Y FORMA DE PAGO:** a) En consideración a los pagos que El PODER JUDICIAL (El Contratante) hará a EL PROVEEDOR como en lo sucesivo se menciona, el PROVEEDOR por este medio se compromete con el PODER JUDICIAL (CONTRATANTE) a ejecutar y completar el Suministro o la entrega y a subsanar cualquier defecto del mismo, de conformidad en todo respecto con los documentos utilizados en el proceso de

contratación. b) EL PODER JUDICIAL (CONTRATANTE) por este medio se compromete a pagar al PROVEEDOR como retribución a la entrega completa del suministro y la subsanación de sus defectos, el Precio del Contrato o aquellas sumas que resulten pagaderas bajo las disposiciones del contrato en el plazo y en la forma establecidas en este. EL PROVEEDOR, se compromete y obliga a hacer las entregas del suministro (bienes o servicios …) descritos en la cláusula …….. precisamente en lo que corresponde a la descripción y especificaciones técnicas, conforme al Calendario de entregas (parciales o totales) lo que forman parte integral del presente contrato; todo por la suma de……lempiras exactos……. (Lps……..) incluyendo el impuesto sobre ventas.- **Forma de Pago** 1) El PODER JUDICIAL (Contratante) pagará a EL PROVEEDOR según las entregas programadas conforme la oferta presentada y previo Informe del Supervisor designado por el Poder Judicial. 2)…….3) Los pagos serán a través de la Pagaduría Especial del Poder Judicial. **CLAUSULA SEPTIMA: VIGENCIA DEL CONTRATO** : El presente Contrato tendrá una vigencia de ……. Meses(…..) a partir del …….al …….de…… del 202……- **CLÁUSULA OCTAVA PENALIDAD:** En caso que EL PROVEEDOR no cumpla con el plazo de entrega establecido para el suministro, se le sancionará de conformidad con lo establecido en los Artículos 3B y 72 de la Ley de Contratación del Estado y numeral …..del documento Base, equivalente al 0.36% en relación con el monto total del saldo del contrato, según lo estable el artículo…… de las Disposiciones Generales para la Ejecución del Presupuesto General de Ingresos y egresos de la República vigente para el año 202---. Lo anterior sin perjuicio de hacer efectiva la Garantía de cumplimiento, procediéndose si así conviene a EL PODER JUDICIAL a la resolución del Contrato, reservándose además el ejercicio de las acciones legales por daños y perjuicios por incumplimiento del contrato por parte de EL PROVEEDOR que procedieren.- **CLAUSULA NOVENA: SUPERVISION**: Para la correcta ejecución del presente Contrato la Supervisión estará a cargo del EL PODER JUDICIAL a través de la Dirección de…….. quien será el encargado de la supervisión del contrato, de vigilar la buena marcha de lo estipulado, obligándose en tal sentido EL PROVEEDOR a cumplir cabalmente las recomendaciones y directrices emanadas del Supervisor, siempre y cuando se refieran a los objetivos del presente Contrato.- **CLÁUSULA DECIMA: GARANTIAS** : EL PROVEEDOR, deberá rendir a favor de EL PODER JUDICIAL las siguientes garantías que deberán ser emitidas por una Institución

Bancaria o Compañía Aseguradora y contendrán indefectiblemente, la cláusula obligatoria siguiente: **"LA PRESENTE GARANTÍA/FIANZA SERA EJECUTADA POR EL MONTO TOTAL DE LA MISMA A SIMPLE REQUERIMIENTO DEL BENEFICIARIO, LA MISMA, ACOMPAÑADA DE UNA RESOLUCION FIRME DE INCUMPLIMIENTO SIN NINGUN OTRO REQUISITO, PUDIENDO REQUERIRSE EN CUALQUIER MOMENTO DENTRO DEL PLAZO DE VIGENCIA DE LA GARANTIA/FIANZA. LA PRESENTE GARANTIA/FIANZA EMITIDA A FAVOR DEL BENEFICIARIO CONSTITUYE UNA OBLIGACION SOLIDARIA, INCONDICIONAL, IRREVOCABLE Y DE EJECUCION INMEDIATA; EN CASO DE CONFLICTO ENTRE EL BENEFICIARIO Y EL ENTE EMISOR DEL TITULO, AMBAS PARTES SE SOMETERAN LA JURISDICCION DE LOS TRIBUNALES DE LA REPUBLICA DEL DOMICILIO DEL BENEFICIARIO. LA PRESENTE CLAUSULA ESPECIAL OBLIGATORIA PREVALECERA SOBRE CUALQUIER OTRA CONDICION"** Siendo esta la siguiente: **1) GARANTÍA DE CUMPLIMIENTO DE CONTRATO**: EL PROVEEDOR deberá rendir una garantía de cumplimiento equivalente al quince por ciento (15%) del valor total de la oferta del suministro a entregar y servirá para garantizar que EL PROVEEDOR, provea el suministro cumpliendo con todas las condiciones estipuladas en el presente contrato, la cual deberá tener una vigencia de tres (3) meses después del plazo previsto para la provisión del suministro. Esta presentación debe coordinarse entre EL PROVEEDOR Y EL Departamento de……..a través del Supervisor con el apoyo de la Unidad de Licitaciones. Asimismo, deberá presentarse la Declaración emitida por la Institución Garante que extendió dicha Garantía. Lo anterior en cumplimiento de los artículos 100,101, 102 y 103 de la Ley de Contratación y 241 y 242 de su Reglamento. **1) GARANTIA DE CALIDAD DEL SUMINISTRO**: El PROVEEDOR otorgará a favor de EL PODER JUDICIAL una garantía equivalente al cinco por ciento (5%) del monto del Contrato por los vicios o defectos del suministro, conforme a lo establecido en el artículo 104 de la Ley de Contratación del Estado. Esta garantía entrará en vigencia a partir de la fecha de inicio del Contrato, con una duración de ……..(---) meses. Mediante esta garantía EL PROVEEDOR se compromete a reponer o reparar por su cuenta cualquier defecto o fallas ocasionadas por las deficiencias de equipos o materiales, mano de obra, equipamiento, vicios ocultos y por cualesquier otros aspectos que le fueren imputables **al**

PROVEEDOR con el propósito de mantener la disponibilidad del servicio en las sedes judiciales objeto del este contrato. **CLÁUSULA UNDECIMA: OBLIGACIONES DEL PROVEEDOR: a)** El Proveedor se obliga a emplear toda su capacidad profesional, técnica, administrativa y económica, a fin de ejecutar cumplidamente el contrato; asi como está estipulado en las especificaciones técnicas; acatando cabalmente las instrucciones y recomendaciones emanadas de la Supervisión, conducentes a la buena prestación del suministro; **b)** Todo gasto que origine la sustitución o reemplazo de piezas o accesorios que resulten defectuosos, así como la reparación o mantenimiento (de proceder)…….correrá por cuenta de EL PROVEEDOR, **c**) Todos los bienes, materiales o accesorios suministrados deben ser nuevos, **d)** Garantizar la prestación de un servicio eficiente mediante la dotación de suministros modernos y funcionales, **e**) Brindar capacitación a los usuarios en uso manejo y cuidados de los suministros (si fuere el caso), **f)** Puntualidad en la entrega de los insumos, suministros…etc. de modo que no se paralice la operatividad de la Institución, **g**) Garantizar diligencia en el servicio de mantenimiento y reparación de los suministros (según el caso), **h)** Subsanar los daños y perjuicios ocasionados a EL PODER JUDICIAL o a terceros que se deriven de las causas antes señaladas, excepto los ocasionados por fuerza mayor o caso fortuito debidamente comprobados y **j)** Todas aquellas obligaciones contenidas en el documento base del proyecto, el cual forma parte integra de este Contrato.- **CLÁUSULA DUODECIMA: CASO FORTUITO O FUERZA MAYOR**: EL Incumplimiento total o parcial del presente contrato porte de EL PROVEEDOR, no serán considerados como tal, si se atribuye a motivos de caso fortuito o fuerza mayor debidamente justificados tales como: **a)** guerra, rebelión y motines, **b)** huelga, excepto aquellas de empleados de EL PODER JUDICIAL (CONTRATISTA); **c)** desastres naturales tales como: terremotos, maremotos, incendios, huracanes e inundaciones y que pongan en peligro la seguridad de los bienes a suministrar. **CLALUSULA DECIMA TERCERA SOLUCION DE CONFLICTOS :** Cualquier controversia o conflicto que se produzca entre las partes, deberá ser resuelta en forma conciliatoria, siempre y cuando no sea lesivo para los intereses del Estado ni contravengan disposiciones legales, caso contrario en la solución de estas controversias deberá realizarse de acuerdo a lo establecido el artículo 3 de la Ley de Contratación del Estado, siendo competencia de la jurisdicción de lo Contencioso Administrativo para dirimir conflictos. **CLÁUSULA DECIMA CUARTA: DOCUMENTOS INTEGRANTES DEL**

CONTRATO.- Forman parte del presente contrato: **1)** Pliego de Condiciones o Documento base; **2)** Especificaciones Técnicas aprobada por el Poder Judicial; **3)** Oferta original del Proveedor ; **5)** Informe de Revisión y Análisis, **6**) Garantías; **7)** Acuerdo de Adjudicación, **8)** Orden de Inicio, **9)** Cualquier otro documento relacionado con la ejecución del presente contrato.- **CLAUSULA DECIMA QUINTA :TERMINACIÓN, Y LIQUIDACIÓN DEL CONTRATO.-** El presente contrato terminará: **a)** por el grave o reiterado incumplimiento de las cláusulas, **b)** La falta de constitución de la Garantía de Cumplimiento de Contrato, **c)** la disolución de la Sociedad Mercantil de EL PROVEEDOR, **d)** La declaración de quiebra o la incapacidad financiera de EL PROVEEDOR, **e)** Los motivos de interés público o las circunstancias imperativas calificadas como caso fortuito o fuerza mayor sobrevinientes a la celebración de este Contrato que imposibiliten o agraven desproporcionadamente su ejecución; **f)** El mutuo acuerdo entre las partes, **g**) por el cumplimiento normal de las prestaciones por ambas partes o por resolución dl mismo, cuando hubiere causas suficientes, todo al tenor de los Artículos 126 al 131 de la Ley de Contratación del Estado, **h)** En cumplimiento a las Disposiciones Generales para la ejecución el Presupuesto General de Ingresos y Egresos de la República vigentes se transcribe el artículo ------ que 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 al 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 pro 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 imprevistos o de emergencia**. Lo dispuesto en este Artículo debe estipularse obligatoriamente en los pliegos de condiciones, bases de licitación, términos de referencia u otros documentos previos a la celebración del contrato y en el contrato mismo del sector público.-. **CLÁUSULA DECIMA SEXTA CESION Y SUBCONTRATACION** : No se aceptará la cesión del contrato y la subcontratación se hará con la autorización expresa de EL PODER JUDICIAL.-**CLAUSULA DECIMA SEPTIMA CONFIDENCIALIDAD**: (si fuera el caso) EL PROVEEDOR se obliga a guardar el secreto profesional respecto a los datos, tanto de carácter empresarial como de carácter personal de terceros vinculados a los que tuviera acceso, obligación que sustituirá aún después de finalizada las relación con EL PODER JUDICIAL y establecerá medidas técnicas y organizativas necesarias que garanticen la seguridad e integridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

De igual manera, los datos podrán ser utilizados única y exclusivamente para la finalidad correcta del servicio contratado por su personal técnico, al momento de tener acceso a los equipos de impresión, para; instalación, configuración, reparación, cambio de equipo y toda manipulación que conozca y que le atañen en esta materia. Siendo EL PROVEEDOR el máximo responsable de cualquier mal uso realizado con la información, en función del servicio prestado; los daños y perjuicios que se ocasionen con motivos del incumplimiento de lo establecido en esta cláusula, será motivo de las acciones legales y administrativas correspondientes. **CLAUSULA DECIMA OCTAVA MODIFICACIONES** Cualquier modificación al contrato se hará de común acuerdo entre las partes, siguiendo el procedimiento establecido en la Ley de contratación del Estado y su Reglamento. **CLAUSULA DECIMA NOVENA: LEY APLICABLE**.- En todo aquello no previsto en este contrato y demás documentos que la conforman, se estará a lo estipulado en la Ley de Contratación del Estado y su Reglamento, Ley de Procedimiento Administrativo, Disposiciones Generales del Presupuesto General de Ingresos y Egresos de la República vigente, Reglamento de Ejecución Presupuestaria del Poder Judicial, documento base y demás leyes aplicables a la materia.- **CLAUSULA VIGESIMA, DE INTEGRIDAD"** Las Partes, en cumplimiento a lo establecido en el Artículo 7 de la Ley de Transparencia y Acceso a la Información Pública (LTAIP), 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 de: **INTEGRIDAD, LEALTAD CONTRACTUAL, EQUIDAD, TOLERANCIA, IMPARCIALIDAD Y DISCRECIÓN CON LA INFORMACIÓN CONFIDENCIAL QUE MANEJAMOS, ABSTENIÉNDONOS DE DAR DECLARACIONES PÚBLICAS SOBRE LA MISMA**. **2.** Asumir una estricta observancia y aplicación de los principios fundamentales bajos los cuales se rigen los procesos de contratación y adquisiciones públicas establecidos en la Ley de Contratación del Estado, tales como: transparencia, igualdad y libre competencia. **3.** Que durante la ejecución del Contrato ninguna persona que actúe 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 indirectamente, cualquier cosa de valor para influenciar las acciones de la otra parte; **b) Prácticas Colusorias:** entendiendo éstas

como aquellas en las que denoten, sugieran o demuestren que existe un acuerdo malicioso entre dos o más partes o entre una de las partes y uno o varios terceros, realizado con la intención de alcanzar un propósito inadecuado, incluyendo influenciar en 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.** 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 derivadas del régimen laboral y, en su caso entablar las acciones legales que correspondan. **b.** Departe 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 que 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, firmando voluntariamente para constancia. - **CLÁUSULA VIGÉSIMA PRIMERA: ACEPTACIÓN DE LAS PARTES. -** Ambas partes aceptan todas las estipulaciones del presente contrato y se obligan a su fiel cumplimiento.

En testimonio de lo cual las partes firman el presente Contrato por duplicado en la ciudad de Tegucigalpa, Municipio del Distrito Central, el día, mes y año antes indicados.

_____ _____

EL PODER JUDICIAL **El PROVEEDOR**

AUTORIZACIÓN DEL

FABRICANTE

[El Oferente solicitará al Fabricante que complete este formulario de acuerdo con las instrucciones indicadas. Esta carta de autorización deberá estar escrita en papel membrete del Fabricante y deberá estar firmado por la persona debidamente autorizada para firmar documentos que comprometan el Fabricante. El Oferente lo deberá incluir en su oferta, si así se establece en los ***DDL****.]*

Fecha: [*indicar la fecha (día, mes y año) de presentación de la oferta]*
LPN No.: *[indicar el número del proceso licitatorio]*
Alternativa No.: *[indicar el No. de identificación si esta es una oferta por una alternativa]*

A: [*indicar el nombre completo del Comprador]*

POR CUANTO

Nosotros *[nombre completo del fabricante]*, como fabricantes oficiales de *[indique el nombre de los bienes fabricados]*, con fábricas ubicadas en *[indique la dirección completa de las fábricas]* mediante el presente instrumento autorizamos a *[indicar el nombre y dirección del Oferente]* a presentar una oferta con el solo propósito de suministrar los siguientes Bienes de fabricación nuestra *[nombre y breve descripción de los bienes]*, y a posteriormente negociar y firmar el Contrato.

Por este medio extendemos nuestro aval y garantiza, conforme a los pliegos de condiciones, respecto a los bienes ofrecidos por la firma antes mencionada.

Firma: _____
[firma del(los) representante(s) autorizado(s) del fabricante]

Nombre: *[indicar el nombre completo del representante autorizado del Fabricante]*

Cargo: [*indicar cargo]*

Debidamente autorizado para firmar esta Autorización en nombre de: *[nombre completo del Oferente]*

Fechado en el día _____ de _____de 20___*[fecha de la firma]*

FORMATO GARANTIA MANTENIMIENTO DE OFERTA

NOMBRE DE ASEGURADORA / BANCO

GARANTIA / FIANZA DE MANTENIMIENTO DE OFERTA Nº _____

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

_____

SUMA AFIANZADA/GARANTIZADA: _____

VIGENCIA De: Hasta: _____ _____

BENEFICIARIO: _____

CLAUSULA ESPECIAL OBLIGATORIA: ***LA PRESENTE GARANTÍA/FIANZA SERA EJECUTADA POR EL MONTO TOTAL DE LA MISMA A SIMPLE REQUERIMIENTO DEL BENEFICIARIO, ACOMPAÑADA DE UNA RESOLUCION FIRME DE INCUMPLIMENTO, SIN NINGUN OTRO REQUISITO, PUDIENDO REQUERIRSE EN CUALQUIER MOMENTO DENTRO DEL PLAZO DE VIGENCIA DE LA GARANTIA/FIANZA. LA PRESENTE GARANTIA/FIANZA EMITIDA A FAVOR DEL BENEFICIARIO CONSTITUYE UNA OBLIGACION SOLIDARIA, INCONDICIONAL, IRREVOCABLE Y DE EJECUCION AUTOMATICA; EN CASO DE CONFLICTO ENTRE EL BENEFICIARIO Y EL ENTE EMISOR DEL TITULO, AMBAS PARTES SE SOMETEN A LA JURISDICCION DE LOS TRIBUNALES DE LA REPUBLICA DEL DOMICILIO DEL BENEFICIARIO. LA PRESENTE CLAUSULA ESPECIAL OBLIGATORIA PREVALECERA SOBRE CUALQUIER OTRA CONDICIÓN***. 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:
Retira su oferta durante el período de validez de la misma.
No acepta la corrección de los errores (si los hubiere) del Precio de la Oferta.
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.
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_____.

_____

FIRMA AUTORIZADA

FORMATO GARANTIA DE CUMPLIMIENTO

ASEGURADORA / BANCO

GARANTIA / FIANZA DE CUMPLIMIENTO Nº: _____

FECHA DE EMISION: _____

AFIANZADO/GARANTIZADO: _____

DIRECCION Y TELEFONO: _____

Fianza / Garantía a favor de _____, 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: "_ ubicado en
SUMA AFIANZADA/ GARANTIZADA: _____

VIGENCIA De: Hasta: _____ _____

BENEFICIARIO: _____

CLAUSULA ESPECIAL OBLIGATORIA: "*LA PRESENTE GARANTÍA/FIANZA SERA EJECUTADA POR EL MONTO TOTAL DE LA MISMA A SIMPLE REQUERIMIENTO DEL BENEFICIARIO, ACOMPAÑADA DE UNA RESOLUCION FIRME DE INCUMPLIMENTO, SIN NINGUN OTRO REQUISITO, PUDIENDO REQUERIRSE EN CUALQUIER MOMENTO DENTRO DEL PLAZO DE VIGENCIA DE LA GARANTIA/FIANZA. LA PRESENTE GARANTIA/FIANZA EMITIDA A FAVOR DEL BENEFICIARIO CONSTITUYE UNA OBLIGACION SOLIDARIA, INCONDICIONAL, IRREVOCABLE Y DE EJECUCION AUTOMATICA; EN CASO DE CONFLICTO ENTRE EL BENEFICIARIO Y EL ENTE EMISOR DEL TITULO, AMBAS PARTES SE SOMETEN A LA JURISDICCION DE LOS TRIBUNALES DE LA REPUBLICA DEL DOMICILIO DEL BENEFICIARIO. LA PRESENTE CLAUSULA ESPECIAL OBLIGATORIA PREVALECERA SOBRE CUALQUIER OTRA CONDICIÓN*".

A las Garantías Bancarias o fianzas emitidas a favor BENEFICIARIO no deberán adicionarse cláusulas que anulen o limiten la cláusula especial obligatoria.

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

_____

FIRMA AUTORIZADA

FORMATO GARANTIA DE CALIDAD

ASEGURADORA / BANCO

GARANTIA / FIANZA DE CALIDAD: _____

FECHA DE EMISION: _____

AFIANZADO/GARANTIZADO: _____

DIRECCION Y TELEFONO: _____

Fianza / Garantía a favor de _____ , para garantizar" la **calidad DE SUMINISTRO** del Proyecto: "_____ ubicado en por el . Construido/entregado Afianzado/Garantizado_.

SUMA AFIANZADA/ GARANTIZADA: _____

VIGENCIA De: Hasta: _____ _____

BENEFICIARIO: _____

"LA PRESENTE GARANTÍA/FIANZA SERA EJECUTADA POR EL MONTO TOTAL DE LA MISMA A SIMPLE REQUERIMIENTO DEL BENEFICIARIO, ACOMPAÑADA DE UNA RESOLUCION FIRME DE INCUMPLIMENTO, SIN NINGUN OTRO REQUISITO, PUDIENDO REQUERIRSE EN CUALQUIER MOMENTO DENTRO DEL PLAZO DE VIGENCIA DE LA GARANTIA/FIANZA. LA PRESENTE GARANTIA/FIANZA EMITIDA A FAVOR DEL BENEFICIARIO CONSTITUYE UNA OBLIGACION SOLIDARIA, INCONDICIONAL, IRREVOCABLE Y DE EJECUCION AUTOMATICA; EN CASO DE CONFLICTO ENTRE EL BENEFICIARIO Y EL ENTE EMISOR DEL TITULO, AMBAS PARTES SE SOMETEN A LA JURISDICCION DE LOS TRIBUNALES DE LA REPUBLICA DEL DOMICILIO DEL BENEFICIARIO. LA PRESENTE CLAUSULA ESPECIAL OBLIGATORIA PREVALECERA SOBRE CUALQUIER OTRA CONDICIÓN".

A las Garantías Bancarias o fianzas emitidas a favor BENEFICIARIO no deberán **adicionarse cláusulas que anulen o limiten la cláusula especial obligatoria.**

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

_____

FIRMA AUTORIZADA

[4] La Garantía de Calidad deberá solicitarse cuando se requiera según la naturaleza de los bienes.

FORMATO DE GARANTIA DE BUEN SUMINISTRO

ASEGURADORA / BANCO

GARANTIA / FIANZA DE BUEN SUMINISTRO: _____

FECHA DE EMISION: _____

AFIANZADO/GARANTIZADO: _____

DIRECCION Y TELEFONO: _____

Fianza / Garantía a favor de: _____ , para garantizar"

En caso de los defectos y/o fallas ocasionadas por deficiencias en materiales, mano de obra, equipamiento y vicios ocultos del suministro del Proyecto: "

Construido/entregado _____

Afianzado/Garantizado _____.

SUMA AFIANZADA/ GARANTIZADA: _____

VIGENCIA De: Hasta: _____ _____

BENEFICIARIO: _____

"LA PRESENTE GARANTÍA/FIANZA SERA EJECUTADA POR EL MONTO TOTAL DE LA MISMA A SIMPLE REQUERIMIENTO DEL BENEFICIARIO, ACOMPAÑADA DE UNA RESOLUCION FIRME DE INCUMPLIMENTO, SIN NINGUN OTRO REQUISITO, PUDIENDO REQUERIRSE EN CUALQUIER MOMENTO DENTRO DEL PLAZO DE VIGENCIA DE LA GARANTIA/FIANZA. LA PRESENTE GARANTIA/FIANZA EMITIDA A FAVOR DEL BENEFICIARIO CONSTITUYE UNA OBLIGACION SOLIDARIA, INCONDICIONAL, IRREVOCABLE Y DE EJECUCION AUTOMATICA; EN CASO DE CONFLICTO ENTRE EL BENEFICIARIO Y EL ENTE EMISOR DEL TITULO, AMBAS PARTES SE SOMETEN A LA JURISDICCION DE LOS TRIBUNALES DE LA REPUBLICA DEL DOMICILIO DEL BENEFICIARIO. LA PRESENTE CLAUSULA ESPECIAL OBLIGATORIA PREVALECERA SOBRE CUALQUIER OTRA CONDICIÓN".

A las Garantías Bancarias o fianzas emitidas a favor BENEFICIARIO no deberán **adicionarse cláusulas que anulen o limiten la cláusula especial obligatoria.**

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

_____

FIRMA AUTORIZADA

República de Honduras

[Poder Judicial]

Perfil del Proyecto **"Renovación Licenciamiento de Software Antivirus para el Poder Judicial"**

Licitación Pública Nacional

[14-2022]

El **Poder Judicial**, invita a la Empresas interesadas en participar en la **Licitación Pública Nacional N°:14-2022** a presentar ofertas selladas para la "**Renovación Licenciamiento de Software Antivirus para el Poder Judicial".**

El financiamiento para la realización del presente proceso proviene de Fondos Propios del Poder Judicial.

La licitación se efectuará conforme a los procedimientos de Licitación PúblicaNacional (LPN) establecidos en la Ley de Contratación del Estado y su Reglamento.

5. Los interesados podrán adquirir los documentos de la presente licitación, , a partir del _____ de _____ de 2022, en un horario de 7:30 a.m. a 4:00 p.m., mediante solicitud escrita a la Unidad de Licitaciones del Poder Judicial, teléfono 2225-9901, ubicada en el edificio que alberga las nuevas oficinas de la Dirección Administrativa y la Unidad de Licitaciones del Poder Judicial en Colonia Miraflores Sur, atrás del Palacio de Justicia, Tegucigalpa, M.D.C., en un horario de 7:30 a.m. a 4:00 p.m., previo al pago **NO REEMBOLSABLE** de doscientos lempiras exactos (L 200.00), en la Pagaduría Especial del Poder Judicial, ubicada en el primer piso del Edificio Administrativo, parte Sur-Occidental del Palacio de Justicia. El método de pago será mediante la cancelación en efectivo. 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).

6. Cualquier consulta, dudas favor presentarlas por escrito, en la oficina de la Unidad de Licitaciones, ubicada en el Edificio que alberga las nuevas oficinas de la Dirección Administrativa y la Unidad de Licitaciones del Poder Judicial en Colonia Miraflores Sur, atrás del Palacio de Justicia, Tegucigalpa, M.D.C., a más tardar el _____ de 202___, último día para hacer las preguntas. Pasada esta fecha, no se aceptarán más consultas según lo preceptuado en el Artículo 105 del Reglamento de la Ley de Contratación del Estado.

7. La recepción y apertura de ofertas serán en acto público en el Salón de Sesiones ubicado en el Edificio que alberga las nuevas oficinas de la Dirección Administrativa y la Unidad de Licitaciones del Poder Judicial en Colonia Miraflores Sur, atrás del Palacio de Justicia, Tegucigalpa M.D.C., el día (Fecha probable de apertura de oferta, dentro de 40 días

después de aprobadas y publicadas las bases) _____ de _____ de 202___, a las 9:00 a.m. Las ofertas que se reciban fuera de plazo serán rechazadas. Las ofertas se abrirán en presencia de los representantes de los Oferentes que deseen asistir en la dirección, fecha y hora indicada. Todas las ofertas deberán estar acompañadas de una Garantía de Mantenimiento de la Oferta del 2% por el monto ofertado y la forma establecidos en los documentos de Licitación.

Tegucigalpa, M.D.C. noviembre, 2022

Unidad de Licitaciones