

CONTRATO DE COMPRA VENTA

FECHA:	28 DICIEMBRE DE 2022	CONTRATO N°:	30047
TIPO ENTREGA:	ENTREGA A PLAZOS	VIGENCIA HASTA:	28/2/2024
NOMBRE OFERTA:	PROCESO No. MB-03/2023 "ADQUISICIÓN Y RENOVACIÓN DE LICENCIAMIENTO PARA BANDESAL Y FONDOS QUE ESTE ADMINISTRA"		
PRODUCTO:	LOTE 1		
UNIDAD:	SEGUN ANEXO	ORIGEN:	INDIFERENE
CANTIDAD:	SEGUN ANEXO	PRECIO UNITARIO US\$:	SEGUN ANEXO
PLAZO ENTREGA:		PLAZO DE PAGO:	30 CORRIDOS
GARANTIA FIEL CUMPLIMIENTO:	10.0 %		
PUESTO DE BOLSA O LICENCIATARIO COMPRADOR:	BOLPROS S.A. DE C.V.		
AGENTE DE BOLSA COMPRADOR:	JUAN CARLOS MARTINEZ SANCHEZ		
N°. CREDENCIAL:	65		
PUESTO DE BOLSA O LICENCIATARIO VENDEDOR:	SERVICIOS BURSATILES SALVADOREÑOS, S.A. ...		
AGENTE DE BOLSA VENDEDOR:	JOSE SALVADOR PORTILLO VELASQUEZ		
N°. CREDENCIAL:	62		
DATOS DE LIQUIDACION MONETARIA			
VALOR NEGOCIADO:	US\$		\$ 59,000.00
IVA S/VALOR NEGOCIADO:	US\$		\$ 7,670.00
TOTAL:	US\$		\$ 66,670.00
OBSERVACIONES:	<p>AL VALOR NEGOCIADO SE DEBE DE INCLUIR LOS IMPUESTOS SEGÚN EL REGIMEN TRIBUTARIO QUE APLIQUE, EL CUAL DEPENDERA DEL SUJETO Y NATURALEZA DEL BIEN NEGOCIADO -- OFERTA DE COMPRA -- 372/2022, VER FORMULARIO DE PRECIOS, ASI MISMO LAS CONDICIONES BURSATILES ESTABLECIDAS SEGÚN LOS CONTRATOS DE COMISIÓN DE LOS PUESTO DE BOLSA O EL CONVENIO POR SERVICIOS DE NEGOCIACIÓN POR CUENTA DEL ESTADO DE LA BOLSA DE PRODUCTOS DE EL SALVADOR</p>		


FIRMA DEL AGENTE COMPRADOR


FIRMA DEL AGENTE VENDEDOR


FIRMA DEL DIRECTOR DE CORRO



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

Nombre de Oferta	PROCESO No. MB-03/2023 "ADQUISICIÓN Y RENOVACIÓN DE LICENCIAMIENTO PARA BANDESAL Y FONDOS QUE ESTE ADMINISTRA"
Producto	ADQUISICIÓN Y RENOVACIÓN DE LICENCIAMIENTO Y SERVICIOS DE SOPORTE
Institución	BANCO DE DESARROLLO DE REPÚBLICA DE EL SALVADOR (BANDESAL)
Precio	<p>SEGUN ANEXO</p> <p>Fondos propios (BANDESAL, FDE y FSG).</p> <p>LOTE 1: Suscripción de plataforma de software de seguridad de Endpoint y servidores US\$ 52,000.00 SIN IMPUESTOS</p>
Cantidad	Ver especificaciones técnicas detalladas en el ANEXO No. 1, ANEXO No. 2, ANEXO No. 3.
Término	<p>Bolsa de Productos de El Salvador, Sociedad Anónima de Capital Variable que en lo sucesivo se denominará la Bolsa.</p> <p>Banco de Desarrollo de la República de El Salvador que en lo sucesivo se denomina BANDESAL.</p> <p>Gerencia de Servicios Institucionales, en lo sucesivo se denominará GSI.</p>
Condiciones de Negociación	<p>Podrán participar en la presente negociación las personas Jurídicas que no se encuentren incapacitadas para ofertar y contratar, impedidas para ofertar y/o inhabilitadas para participar y contratar con la Administración Pública. FORMATO No. 1.</p> <p>La negociación se realizará por lote completo.</p> <p>El orden de la rueda de negociación será por el orden de los lotes.</p> <p>Cláusula de no colusión</p> <p>Tres (3) días hábiles antes de la negociación, se deberá entregar a la Bolsa de Productos de El Salvador, Sociedad Anónima de Capital Variable, una Declaración Jurada ante notario (Ver FORMATO No. 3) en la que manifieste que no ha constituido acuerdos colusorios con uno, varios o todos los demás ofertantes que participan en el presente proceso, y que constituyan violación al Lit. c) del artículo veinticinco de la ley de competencia según el modelo de declaración jurada establecido en el mecanismo bursátil.</p> <p>Los datos generales del proveedor (Formato N° 4) serán presentados por el puesto vendedor a GSI/BOLPROS, anexada al comprobante de presentación de ofertas técnicas. Esta información deberá ser incorporada en formato digital en el sistema de seguimiento de ofertas denominado TOFF, que BOLPROS ha puesto a disposición; a más tardar el siguiente día hábil después de finalizado el plazo de presentación de ofertas técnicas.</p>



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

	Los números de contratos del Formato N° 8, Formato N° 10, y Formato N° 14 serán agregados por el agente delegado posterior al cierre.															
Especificaciones Técnicas	Según Especificaciones Técnicas detalladas en ANEXO No. 1, ANEXO No. 2, ANEXO No. 3.															
Origen	Indiferente															
Fecha, volumen, horario y lugar de entrega	<p>Plazo de entrega.</p> <p>El plazo máximo para la entrega será contado a partir del día siguiente al cierre del contrato, de acuerdo con lo siguiente:</p> <p>Para LOTE 1:</p> <table border="1" style="margin-left: 40px;"> <thead> <tr> <th>Tiempo límite de Entrega</th> <th>Equipos por entregar</th> <th>Documentos para la entrega</th> </tr> </thead> <tbody> <tr> <td>31/12/2022</td> <td>Adquisición de Suscripciones de software de solución de seguridad de Endpoint.</td> <td>Acta de recepción</td> </tr> <tr> <td>31/12/2022</td> <td>Adquisición de suscripciones de software de seguridad avanzada para Servidores.</td> <td>Acta de recepción</td> </tr> <tr> <td>13/01/2023</td> <td>Instalación de la solución ofertadas.</td> <td>Acta de recepción</td> </tr> <tr> <td>31/12/2022</td> <td>Soporte local 24x7 con Ingenieros Certificados en la solución ofertada.</td> <td>Acta de recepción</td> </tr> </tbody> </table> <p>Lugar de entrega del suministro será: en Calle El Mirador y 89 avenida norte, Edificio World Trade Center II, Nivel 4, Col. Escalón, San Salvador.</p> <p>Horario de entrega: Deberá coordinarse previamente con el Administrador del Contrato.</p> <p>Las solicitudes de modificación al plazo de entrega, instalación y configuración por razones de caso fortuito o fuerza mayor, deberá ser solicitado por escrito a la Bolsa, seis (6) días hábiles de anticipación a la fecha pactada en el contrato adjuntando las justificaciones y comprobaciones correspondientes y serán aprobadas por el Administrador de contrato en los casos que el comprador, no se vea afectado en su operatividad.</p> <p>Para la entrega se emitirá un Acta de Recepción, la cual deberá ser firmada por el vendedor y el Administrador de contrato que designe el banco de dicho proceso.</p> <p>Orden de Entrega se deberá presentar para firma y sello del Administrador del Contrato al finalizar la entrega del suministro y luego se deberá presentar en BOLPROS para su liquidación.</p>	Tiempo límite de Entrega	Equipos por entregar	Documentos para la entrega	31/12/2022	Adquisición de Suscripciones de software de solución de seguridad de Endpoint.	Acta de recepción	31/12/2022	Adquisición de suscripciones de software de seguridad avanzada para Servidores.	Acta de recepción	13/01/2023	Instalación de la solución ofertadas.	Acta de recepción	31/12/2022	Soporte local 24x7 con Ingenieros Certificados en la solución ofertada.	Acta de recepción
Tiempo límite de Entrega	Equipos por entregar	Documentos para la entrega														
31/12/2022	Adquisición de Suscripciones de software de solución de seguridad de Endpoint.	Acta de recepción														
31/12/2022	Adquisición de suscripciones de software de seguridad avanzada para Servidores.	Acta de recepción														
13/01/2023	Instalación de la solución ofertadas.	Acta de recepción														
31/12/2022	Soporte local 24x7 con Ingenieros Certificados en la solución ofertada.	Acta de recepción														
Garantías	<p>Los proveedores deberán presentar las siguientes Garantías:</p> <p>✓ Garantía Mantenimiento de Oferta: del 2 % + IVA del valor ofertado.</p> <p>Posterior al cierre de contrato, el proveedor que resulte ganador deberá presentar:</p> <p>✓ Garantía Fiel Cumplimiento de Contrato: del 10% + IVA del valor contratado.</p>															

Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

	<p>La Garantía de fiel cumplimiento debe ser por el plazo del contrato más treinta (30) días calendarios adicionales de conformidad con lo establecido en el Instructivo de Garantías de La Bolsa.</p> <p>Las Garantías de Mantenimiento de Oferta y Fiel Cumplimiento del Contrato se deberán de emitir a favor de la Bolsa de Productos de El Salvador, Sociedad Anónima de Capital Variable, Bolsa de Productos y Servicios que puede abreviarse BOLPROS, S.A. de C.V. Bolsa de Productos y Servicios y serán devueltas una vez se cumpla con los términos del contrato.</p> <p>La garantías podrán constituirse a través de Fianzas otorgadas a favor de La Bolsa, y emitidas por afianzadoras, aseguradoras o Bancos autorizadas por la Superintendencia del Sistema Financiero, cheques certificados o cheque de caja, librado contra un Banco regulado por la Ley de Bancos o de Bancos Cooperativos y Sociedades de Ahorro y Crédito, los cuales deberán ser depositados a la cuenta a nombre de Bolsa de Productos de El Salvador, Sociedad Anónima de Capital Variable No. 1301-13795 del Banco Cuscatlán.</p>
<p>Penalización económica y ejecución coactiva</p>	<p>PENALIZACION POR ENTREGA EXTEMPORANEA.</p> <p>En el caso que el proveedor entregue los productos o brinde el servicio fuera del plazo establecido en el Contrato y sus Anexos, junto con la documentación requerida para la entrega, el Cliente Comprador podrá permitir la entrega fuera de los plazos establecidos en el contrato, y aplicará una penalización CERO PUNTO UNO POR CIENTO (0.1 %) sobre el monto de lo entregado con atraso, por cada día de extemporaneidad.</p> <p>El plazo para poder entregar con extemporaneidad aplicando la penalización antes indicada no podrá exceder a quince (15) días calendario, posteriores a la fecha original de entrega, según contrato.</p> <p>En todo caso, la penalización mínima a imponer relacionada con la entrega de productos será el equivalente a medio salario mínimo del sector comercio; y la penalización mínima a imponer relacionada con la prestación de servicios será el equivalente a un salario mínimo del sector comercio.</p> <p>Penalización que deberá ser calculada por la institución y notificada directamente al proveedor, con copia a la GSI; cancelada por el proveedor directamente en las oficinas de BANDESAL; dentro de los cinco días calendarios siguientes de la notificación de la GSI, por medio de la cual se le comunicó la imposición de la penalización.</p> <p>Para iniciar la gestión de cobro con la entidad compradora debe adjuntarse el recibo de pago de la penalización si la hubiere y además deberá considerarse la fecha de corte de recepción de documentos a cobro por parte la entidad compradora para la emisión del quedan correspondiente.</p> <p>EJECUCION COACTIVA POR PRODUCTOS Y SERVICIOS NO ENTREGADOS.</p> <p>En caso que los productos o servicios no sean entregados, en el plazo original o vencidos los quince días arriba indicados para entregar en forma extemporánea, con penalización, el Puesto de Bolsa Comprador deberá solicitar a la Bolsa que efectúe la</p>



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

	<p>ejecución coactiva del contrato por lo no entregado, de conformidad a los Art. 79 y siguientes del Instructivo de Operaciones y Liquidaciones de la Bolsa de Productos de El Salvador, S.A. de C.V.; dicha solicitud deberá ser dirigida al Gerente General de BOLPROS, S.A. DE C.V., y deberá contener la información relativa al número de contrato, cantidades incumplidas, monto equivalente al incumplimiento, y toda aquella información que permita establecer, identificar y cuantificar el incumplimiento.</p> <p>Los cinco (5) días hábiles para solicitar la ejecución coactiva por lo no cumplido, se contarán a partir de la fecha límite de entrega original acordada contractualmente o a partir del último día del plazo concedido con penalización; conforme a lo dispuesto en los art. 79 y siguientes del Instructivo de Operaciones y Liquidaciones.</p> <p>Será obligatorio para los Puestos de Bolsa contratantes, que, en caso de existir acuerdos entre las partes, dichos acuerdos sean informados a la Bolsa, antes de la realización de las nuevas ruedas de negociación en virtud de la ejecución coactiva; caso contrario la Bolsa continuará con el proceso de ejecución hasta la liquidación de la garantía.</p>
<p>Documentación para tramitar cobro y Fecha de pago de anticipos y de productos o servicios</p>	<p>FACTURACIÓN DIRECTA:</p> <p>El Banco de Desarrollo de la República El Salvador (BANDESAL) podrá solicitar que algunos lotes sean facturados mensualmente a cualquiera de los fondos que éste administra siendo estos: El Fondo de Desarrollo Económico (FDE) y el Fondo Salvadoreño de Garantías (FSG), tanto BANDESAL como FDE y FSG tienen sus propios registros fiscales que serán enviados a la empresa seleccionada.</p> <p>Fondos Propios: Comprobante de Crédito Fiscal a nombre de BANDESAL (NIT 0614-220911-111-0 y NRC 213889-7), Fondo de Desarrollo Económico (NIT 0614-220911-113-7 y NRC 213893-7), Fondo Salvadoreño de Garantía (NIT 0614-220911-112-9 y NRC 213891-0) con las especificaciones detalladas según BANDESAL.</p> <p>La forma de pago será la siguiente:</p> <p>Para LOTE 1: 100% del valor total entregado, al entregar la carta de activación y acreditación del servicio.</p> <p><u>DOCUMENTACIÓN OBLIGATORIA PARA COBRO:</u></p> <p>El proveedor deberá presentar en las Instalaciones del BDES los siguientes documentos:</p> <ol style="list-style-type: none">Acta de recepción, debidamente firmada por la Administrador del Contrato y proveedor del bien o servicio.Comprobante de Crédito Fiscal con las especificaciones detalladas según BANDESAL.Orden de entrega emitida por BOLPROS, la cual deberá ser presentada al finalizar la entrega de la totalidad del suministro, para firma y sello del administrador del contrato y presentada a la Bolsa para su liquidación. <p>Cumplidos los requisitos anteriores, el Banco procederá a efectuar los pagos a más tardar treinta (30) días calendario, después de la fecha de emisión de quedan.</p> <p>El quedan será gestionado en las oficinas de BANDESAL en el local 109.</p>

Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

Otras Condiciones	<p>El Administrador de Contrato de la institución compradora será responsable de verificar la ejecución y cumplimiento de las obligaciones contractuales, derivadas de las presentes Condiciones de la Negociación.</p> <p>El Puesto de Bolsa Vendedor deberá presentar al finalizar la negociación los precios de cierre de conformidad al FORMATO No.8 para el LOTE 1, FORMATO No. 10 para el LOTE 2 y FORMATO No. 14 para el LOTE 3. Estos deberán ser expresados a dos (2) decimales con IVA. <u>Caso contrario, la Institución se reserva el derecho de considerar únicamente los dos (2) primeros decimales, o cuando proceda, aproximará el segundo decimal al número inmediato superior siempre que el tercer decimal sea igual o mayor que cinco.</u></p> <p>Las solicitudes de modificación a los plazos de entrega por razones de caso fortuito o fuerza mayor deberán ser solicitadas por escrito al Puesto de Bolsa Representante del Comprador, con seis (6) hábiles de anticipación a la fecha pactada Si el último día en que debe hacerse la entrega correspondiente fuere asueto, día no hábil o feriado legalmente, se harán las entregas el día siguiente hábil.</p> <p>Después de cerrados los contratos, la GSI comunicará a los Puestos representantes de los Vendedores el nombre del Administrador de Contrato.</p>
Vigencia del Contrato	A partir del cierre de la negociación hasta el 28/02/2024.
Prórrogas y adendas al contrato	De acuerdo con el Art. 82, 83 y 86 del Instructivo de Operaciones y Liquidaciones de La Bolsa.

ESPECIFICACIONES TECNICAS/CONDICIONES ESPECIALES

LOTE	ITEM	CANT.	UNIDAD	DESCRIPCIÓN
1	1	350	S.G.	Crowdstrike Falcon Endpoint Protection Enterprise. Prevent Insight. Threat Graph Standard. Período de vigencia: 1 de enero al 31 de diciembre de 2023
	2	45	S.G.	Crowdstrike Falcon Server Protection. Server Threat Graph Standard. Período de vigencia: 1 de enero al 31 de diciembre de 2023.
	3	120	S.G.	Crowdstrike Falcon Endpoint Protection Pro. Prevent. Período de vigencia: 1 de enero al 31 de diciembre de 2023.
	4	350	S.G.	Crowdstrike Falcon Firewall Management. Período de vigencia: 1 de enero al 31 de diciembre de 2023.
	5	1	Servicios	Implementación
	6	1	Servicios	Soporte local 24x7 con Ingenieros Certificados en la solución ofertada. Período de vigencia: 1 de enero al 31 de diciembre de 2023.



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

ANEXO No. 1

ESPECIFICACIONES TÉCNICAS PARA EL LOTE 1

1. REQUERIMIENTO

El Banco de Desarrollo de la República de El Salvador requiere de Software de Seguridad de equipos Endpoint y Servidores.

2. DETALLE DE LAS UNIDADES A ADQUIRIR:

ITEM	CANT.	UNIDAD	DESCRIPCIÓN
1	350	S.G.	CrowdStrike Falcon Endpoint Protection Enterprise. Prevent Insight. Threat Graph Standard. Período de vigencia: 1 de enero al 31 de diciembre de 2023.
2	45	S.G.	CrowdStrike Falcon Server Protection. Server Threat Graph Standard. Período de vigencia: 1 de enero al 31 de diciembre de 2023.
3	120	S.G.	CrowdStrike Falcon Endpoint Protection Pro. Prevent. Período de vigencia: 1 de enero al 31 de diciembre de 2023.
4	350	S.G.	CrowdStrike Falcon Firewall Management. Período de vigencia: 1 de enero al 31 de diciembre de 2023.
5	1	Servicios	Implementación
6	1	Servicios	Soporte local 24x7 con Ingenieros Certificados en la solución ofertada. Período de vigencia: 1 de enero al 31 de diciembre de 2023.

3. CONDICIONES GENERALES PARA:

Los proveedores deberán cumplir al 100% con lo solicitado en la presente oferta de compra, de lo contrario no serán elegibles para pasar a la rueda de negociación.

4. METODOLOGÍA DE EVALUACIÓN:

La evaluación contempla dos etapas cuyo análisis será realizado por el Banco, el detalle es el siguiente:

FASE	ASPECTOS A EVALUAR	EVALUACION
FASE 1	ASPECTOS LEGALES	CUMPLE / NO CUMPLE
FASE 2	ASPECTOS TECNICOS	CUMPLIMIENTO TOTAL

α) FASE 1 ASPECTOS LEGALES: CUMPLE/NO CUMPLE

CUMPLIMIENTO EN LA PRESENTACIÓN DE DOCUMENTOS:

Se evaluará el cumplimiento de los ofertantes en la presentación de los documentos legales y administrativos, detallados en este anexo. La omisión, error o incumplimiento parcial en la presentación de esta documentación requerida por el Banco es subsanable.

Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

Se establece hasta un plazo máximo de **tres (3) días hábiles** para subsanarlas, después de notificado. Si la documentación no es enviada de conformidad y en el tiempo indicado, automáticamente se excluirá la oferta, por lo que no pasará a la rueda de negociación.

b) FASE 2 ASPECTOS TÉCNICOS: 100.00%

Para la fase de aspectos técnicos se evaluará el cumplimiento de lo requerido en **ANEXO No.1 ESPECIFICACIONES TÉCNICAS** del suministro requerido.

El ofertante deberá presentar en la oferta técnica el **FORMATO No. 5** y dejar claro si cumple o no cumple, dicha oferta deberá estar sujeta al cumplimiento del artículo 19 del Instructivo de Operaciones y Liquidaciones, ya que pueden ofertar igual o superior condiciones o especificaciones detalladas en la presente oferta de compra.

5. DOCUMENTACIÓN OBLIGATORIA PARA PRESENTAR EN LA OFERTA TÉCNICA:

Con el propósito de conocer cuáles ofertantes cumplen con los requerimientos y condiciones de la institución compradora para poder negociar, se solicita la siguiente documentación técnica, la cual es de carácter obligatoria:

Los participantes presentarán la documentación de sus ofertas en original en un sobre cerrado, rotulado así **OFERTA DE COMPRA No. **/2022** denominada **MB-03/2023 “ADQUISICIÓN Y RENOVACIÓN DE LICENCIAMIENTO PARA BANDESAL Y FONDOS QUE ESTE ADMINISTRA”**

Todos los documentos de las ofertas deben ser, distribuidos en el orden y contenido siguiente:

A. DOCUMENTOS ADMINISTRATIVOS/LEGALES

- a) Solvencia Fiscal original o electrónica de la Dirección General de Impuestos Internos, vigente a la fecha de presentación de la oferta.
- b) Declaración Jurada, en acta notarial (**apegarse al FORMATO No. 1**)
- c) Declaración Jurada de Gestión de la seguridad de la información y planes de continuidad del negocio, en acta notarial (**apegarse al FORMATO No. 2**)
- d) Formulario de Identificación del Ofertante (**apegarse al FORMATO No. 4**)
- e) Copia simple de NIT y Tarjeta de Contribuyente del IVA de la Sociedad, indicando la categoría de contribuyente.
- f) Fotocopia simple de DUI y NIT del Representante Legal o Apoderado. Si se tuviere DUI homologado a NIT, presentar solamente Fotocopia simple de DUI homologado del Representante Legal o Apoderado.
- g) Copia certificada por notario del poder que le faculta como apoderado administrativo o Representante Legal de la sociedad.

BANDESAL se reserva el derecho de verificar la documentación recibida y de encontrarse documentación con información que no coincida con la Declaración Jurada (**FORMATO No. 1**) se podrá descalificar la oferta. Adicionalmente los ofertantes deberán cumplir con la Política de Conocimiento del Proveedor de BANDESAL.

B. DOCUMENTOS TÉCNICOS:

1. Carta emitida por el fabricante de la marca ofertada debidamente apostillada (original), en la que manifieste que la empresa oferente es distribuidor autorizado para comercializar



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

los productos y servicios indicando nivel de partner, o en su defecto presentar copia digital de la carta emitida por el fabricante notariada y firmada por el representante legal.

2. Presentación del Formato No. 5- ESPECIFICACIONES TÉCNICAS DEL LOTE 1, donde manifiesta cumplir al 100% los servicios requeridos.
3. Presentación de al menos una (1) carta de referencia con calificación EXCELENTE de empresas a las que haya brindado suministro y configurado las suscripciones del software de seguridad de equipos de la marca ofertada en este proceso en los últimos 5 años (2022,2021,2020,2019, 2018), ver Formato No. 6- MODELO DE CARTA DE REFERENCIA LOTE 1. No se tomarán en cuenta referencias que no sean presentadas en este formato.
4. Presentación del Formato No. 7- PERFIL DEL PERSONAL TÉCNICO ASIGNADO LOTE 1. Que detalle al menos tres (3) técnicos certificados en Administración y/o configuración de la marca y software ofertado, al menos dos (2) técnicos de los presentados deberán haber realizado instalación del servicio en un período máximo de 5 años. Incluir la documentación probatoria de las certificaciones y/o cursos tomados por cada uno de los técnicos detallados en dicho Anexo.

6. NEGOCIACIÓN DEL SUMINISTRO

El ofertante que haya cumplido la totalidad de lo solicitado en el **Anexo No.1**, pasará a la rueda de negociación en la Bolsa de Productos de El Salvador, S. A. de C. V. (BOLPROS), la negociación se realizará en forma total.

7. ADMINISTRADOR DEL SUMINISTRO

El administrador del suministro será el Soporte Técnico de la Unidad de Soporte de la Gerencia de Tecnología, quien actuará en representación del Banco y será el responsable de velar por el cumplimiento del requerimiento y del control del vencimiento del mismo.



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

FORMATO No. 2

MODELO DE DECLARACION JURADA-GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y PLANES DE CONTINUIDAD DEL NEGOCIO

MB-03/2023

ADQUISICIÓN Y RENOVACIÓN DE LICENCIAMIENTO PARA BANDESAL Y FONDOS QUE ESTE ADMINISTRA

En la ciudad de _____, a las _____ horas del día _____ dos mil _____. Ante mí, _____, Notario(a), del domicilio de _____, comparece _____, de ____ años de edad, (ocupación) _____, del domicilio de _____ a quien conozco e identifiqué por medio de su _____; actuando en su carácter de Representante Legal (o apoderado) de la Sociedad _____ (en caso de ser persona natural, se consignara que actúa en su carácter personal o por medio de apoderado), (si es sociedad: sociedad de nacionalidad ____ y del domicilio de _____, con Número de Identificación Tributaria _____); Y ME DICE BAJO JURAMENTO: Que cuenta con un programa o gestión de la seguridad de la información, así como también con una gestión y planes de continuidad del negocio, pruebas desarrolladas y resultados de las pruebas, así mismo, que se verifica la capacidad para recuperar y reanudar el servicio ante interrupciones. Así se expresó el compareciente, a quien expliqué los efectos legales de la presente Acta Notarial la cual consta de ____ hojas útiles y leído que le fue por mí todo lo escrito en un solo acto sin interrupción, manifestó su conformidad, ratificó su contenido y firmamos. DOY FE.

NOTA: Esta declaración jurada deberá ser presentada con todas las formalidades de una Acta Notarial y no deberá de eliminarse ningún literal.



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

FORMATO No. 5 ESPECIFICACIONES TÉCNICAS DEL LOTE 1

Suscripción de plataforma de software de seguridad de Endpoint y servidores

ITEM	CANT.	UNIDAD	DESCRIPCIÓN
1	350	S.G.	CrowdStrike Falcon Endpoint Protection Enterprise. Prevent Insight Threat Graph Standard Período de vigencia: 1 de enero al 31 de diciembre de 2023
2	45	S.G	CrowdStrike Falcon Server Protection. Server Threat Graph Standard Período de vigencia: 1 de enero al 31 de diciembre de 2023
3	120	S.G	CrowdStrike Falcon Endpoint Protection Pro Prevent Período de vigencia: 1 de enero al 31 de diciembre de 2023
4	350	S.G	CrowdStrike Falcon Firewall Management Período de vigencia: 1 de enero al 31 de diciembre de 2023
5	1	Servicios	Implementación
6	1	Servicios	Soporte local 24x7 con Ingenieros Certificados en la solución ofertada. Periodo de vigencia: 1 de enero al 31 de diciembre de 2023.

El ofertante deberá colocar la palabra cumple o no cumple en cada ítem solicitado:

Para el ítem 1, ítem 3 y ítem 4: Se requiere las siguientes especificaciones:

SERVICIOS REQUERIDOS		CUMPLE / NO CUMPLE	# de Pagina
1. Requerimientos técnicos del software			
1	Se requiere que la solución que proponga esté posicionada dentro del cuadrante de "LIDERES" en Gartner 2021 "Magic Quadrant for Endpoint Protection Platforms" Presentar evidencia		
2	Se requiere que la solución pueda ofrecer capacidades de antimalware, control de aplicaciones, reputación web, administración de firewall de Windows, protección de vulnerabilidades mediante parchado virtual, machine learning, protección de amenazas sin archivos (fileless) y capacidad de Detección y respuesta (EDR). Todo en un solo agente que puede ser administrado desde una consola en la nube o local.		
3	Se requiere la solución pueda implementarse de forma local (On-Premise), en la nube (as a Service) o de forma híbrida. Se aclara que solo en el caso de los servidores sin virtuales On-Premise		



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

4	Permitir la integración con Active Directory aún si el equipo en donde se instalará una consola de administración antivirus no se encuentra en el dominio.		
5	Permitir generar un análisis, listado de equipos que cuenten o no con una protección antimalware, basado en dominios o grupos del Active Directory.		
6	*		
7	Permitir a los clientes del árbol de directorios del antivirus, sea un reflejo del árbol de directorios de Active Directory.		
8	La solución deberá tener un agente único conectado a la consola central para todas las características descritas en este documento.		
9	La consola de administración deberá ser centralizada para gestionar a todos los puntos finales sin importar la ubicación geográfica de los mismos.		
10	La administración deberá poderse realizar desde cualquier lugar y con cualquier equipo que soporte un navegador como Firefox o google Chrome por mencionar algunos.		
11	La consola de administración deberá de ser accesible por los puntos finales en cualquier red del Banco e incluso cuando se encuentren conectados a redes públicas sin necesidad de conexión VPN.		
12	La consola deberá contar con un reporte de auditoría de la misma, accesos, actividades, entre otros.		
13	La comunicación entre los agentes y el servidor deberá utilizar un túnel de seguridad SSL/TLS cifrado.		
14	La consola de administración deberá centralizar la administración de los sistemas operativos Windows, MacOS y Linux		
15	La solución antivirus debe proteger a los siguientes sistemas operativos, puestos de trabajo fijos y móviles (portátiles) en las plataformas Intel y AMD, los sistemas operativos: Windows 7, Windows 10, 11 y Sistemas Mac OS		
16	Habilitar o deshabilitar el firewall de acuerdo a la ubicación física de usuario, así como personalización de las políticas o excepciones.		
17	Personalización de opciones de escaneo y Acción para una detección en los modos: Manual, en Tiempo Real y Programado.		
18	Deberá tener la capacidad de crear grupos con la finalidad de ser utilizados en la definición de políticas al menos por dominio, Sistema Operativo, Unidad Organizacional, versión del agente, tipo de equipo de manera independiente.		
19	Importar o Exportar configuraciones de políticas de un grupo de estaciones de trabajo a otro.		



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

20	El agente para equipos Windows deberá soportar de forma automática equipos Servidores y Workstations de 32 y 64 bits, además que el mismo agente podrá ser instalado en equipos físicos, virtuales, VDI y Cloud, dando la misma funcionalidad en cualquiera de ellos.		
21	La consola de administración deberá soportar administración por roles		
22	Se requiere de al menos una semana de almacenamiento de todos los datos generados por los puntos finales sin importar la cantidad de bytes utilizados		
23	La consola de administración debe encontrarse alineada al MITRE ATT&CK FRAMEWORK		
24	La solución deberá contar con una herramienta antivirus de próxima generación con la capacidad hacer frente a las nuevas tácticas, técnicas y procedimientos empleados por los grupos de cibercrimen detrás de los ataques informáticos actuales.		
25	La solución de antivirus deberá contar con un sistema basado en la reputación de sitios web del fabricante de la solución, que permitan de manera proactiva evitar que los usuarios cuando naveguen descarguen componentes maliciosos e infecten sus estaciones de trabajo		
26	La solución debe proveer manejo de niveles de seguridad para evitar la navegación Web a sitios maliciosos cuando los usuarios se encuentran dentro y fuera de la red del Banco. La solución debe permitir reclasificación o recategorización de los sitios web		
27	La solución deberá permitir editar la lista de URL para permitir acceso a URL's que se encuentran bloqueadas (razón sitio de mala reputación o interna) a nivel general, grupos o personal.		
28	*		
29	La solución debe detectar, analizar y eliminar programas maliciosos, como virus, spyware, gusanos, troyanos, keyloggers, programas publicitarios, rootkits, phishing, entre otros.		
30	La solución debe ser capaz de enviar a cuarentena archivos que sean detectados como sospechosos para evitar la ejecución de un archivo malicioso.		
31	La solución debe detectar, analizar y eliminar, de forma automática y en tiempo real, los programas maliciosos en: a. procesos que se ejecutan en la memoria principal (RAM); b. archivos creados, copiar, renombrar, mover o modificados, incluyendo períodos de sesiones en la línea de comandos (DOS o shell) abiertos por el usuario; c. archivos comprimidos de forma automática, al menos en los siguientes formatos: ZIP, EXE, ARJ, MIME / UU, CAB de Microsoft, Microsoft Comprimir. d. archivos recibidos a través de software de comunicación instantánea (MSN Messenger, Yahoo Messenger, Google Talk, ICQ, entre otros). e. Detectar y proteger a la estación de trabajo contra acciones		

Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

	<p>maliciosas que se ejecutan en navegadores Web mediante secuencias de comandos en lenguajes tales como JavaScript, VBScript / ActiveX, etc.</p> <p>f. La detección heurística de virus desconocidos.</p> <p>Debe ser capaz analizar procesos en ejecución, analizar sus distintas características y realizar bloqueos de scripts maliciosos como los siguientes:</p> <p>a.Cscript b.Jar c.Powershell d.Vbs e. Wscript</p>		
32	La solución Antimalware deberá evitar una infección provocada por la ejecución del archivo Autorun.inf contenido en un dispositivo de USB al momento de ser conectado en la estación de trabajo.		
33	La solución deberá monitorear o evitar que un programa con comportamiento sospechoso pueda duplicar o inyectar archivos de sistema similares.		
34	La solución deberá monitorear o evitar que un programa con comportamiento sospechoso pueda modificar el archivo de HOST.		
35	El control de aplicaciones debe contar con una lista de software reconocido como seguro para permitir dichas aplicaciones si se desea. Capacidad de crear reglas en base a un hash, ruta, certificado, software conocido como seguro.		
36	La solución deberá monitorear o evitar que un programa con comportamiento sospechoso pueda incrustar elementos "plug-ins" en el navegador de internet explorer.		
37	La solución deberá monitorear o evitar que un programa con comportamiento sospechoso pueda instalar librería del programa malicioso.		
38	El control de aplicaciones debe tener la capacidad de hacer un whitelisting de las aplicaciones instaladas y no permitir la ejecución de ningún otro software no reconocido.		
39	*		
40	La solución deberá monitorear o evitar que un programa con comportamiento sospechoso instale nuevos servicios. La solución deberá monitorear o evitar que un programa con comportamiento sospechoso modifique archivos de sistema. La solución deberá monitorear o evitar que un programa con comportamiento sospechoso instale servicios o programas para iniciarse al arrancar la estación de trabajo.		
41	Para aquellos programas válidos y que por su comportamiento el Antimalware no permita su ejecución, deberá de permitirlos agregándolos a una lista blanca.		



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

42	Para aquellos programas que no están permitidos ser ejecutados en la estación de trabajo, deberán ser agregados a una lista de bloqueo de programas específicos.		
43	La solución debe ofrecer la capacidad de hacer búsqueda sobre todos los endpoints conectados de indicadores de compromiso.		
44	Se debe poder aislar endpoints para detener propagación de amenazas como parte de la respuesta a un incidente		
45	Capacidad de enviar un mensaje de notificación en la computadora del cliente.		
46	Capacidad de guardar en el log los eventos de control de dispositivos. El almacenamiento de los log de la plataforma Endpoint Protección deberá ser de un mínimo de 7 de registros que debe mostrarse en la consola.		
47	La solución deberá contar como mínimo los siguientes elementos de análisis y características:		
47.1	Aprendizaje de máquina (machine learning en inglés) con características de análisis de archivos previos a su ejecución utilizando algoritmos matemáticos para su identificación, con características de análisis de archivos durante su ejecución que verifique comportamientos, que reduzcan los falsos positivos de forma local en cada punto final con Sistema operativo Microsoft Windows y MacOS		
47.2	La solución deberá contar con tecnología de detección proactiva de virus (Machine Learning), para detectar variantes de virus con características comunes, sin ningún tipo de actualización de firmas. Dicha tecnología deberá contar con componentes de modelado de archivos, los cuales permitan analizar características del archivo como encabezados y deberá contar con un componente que realice análisis dinámico cuando el archivo es ejecutado.		
47.3	Aprendizaje máquina configurable de forma independiente para detectar y para prevenir ataques, de tal forma que pueda tener visibilidad agresiva pero los parámetros de bloqueo moderados, por ejemplo.		
47.4	Inteligencia Artificial.		
47.5	Integración con Virus total		
47.6	Bloqueo de procesos identificados por la inteligencia del fabricante como maliciosos.		
47.7	Definir listas blancas por archivos y/o carpetas.		
47.8	Capacidad de definir múltiples hashes en la lista blanca o lista negra en un solo paso		
47.9	Detección y prevención de scripts o comandos maliciosos vía powershell o CMD incluyendo al menos lo siguiente: Cadenas escritas en una ventana de comandos		

Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

47.1 0	Detección y prevención de intentos de borrado de respaldos del sistema (volume shadow copy por sus siglas en inglés) comúnmente realizado por ataques de ransomware.		
47.1 1	Detección y prevención de ransomware.		
47.1 2	Detección y prevención de los procesos de cifrado de archivos relacionados a extensiones usadas por ransomware.		
47.1 3	Detección y prevención de procesos asociados a accesos indiscriminados al sistema de archivos asociados a ransomware.		
47.1 4	La solución deberá poder identificar comportamientos asociados a dicha amenaza durante su ejecución y frenarlos, tal es el caso de procesos de cifrado no autorizado de archivos.		
47.1 5	*		
47.1 6	Detección y prevención de movimientos laterales.		
47.1 7	Detección y prevención de intentos de robo de credenciales.		
47.1 8	Detección y prevención de intentos de elevación de privilegios.		
47.1 9	Detección y prevención de intentos de uso de "sticky keys"		
47.2 0	Detección y prevención de intentos de ejecución de archivos sospechosos y/o código malicioso creados por los programas de navegación a internet (web browsers por sus siglas en inglés)		
47.2 1	Detección y prevención de intentos de ejecución de rutinas de javascript por línea de comandos vía rundll32.exe		
47.2 2	Los agentes deberán instalarse y funcionar de forma inmediata sin la necesidad de reinicio.		
47.2 3	Se requiere que la solución no esté basada en firmas, de tal forma que los equipos no tengan que recibir diariamente actualizaciones de definiciones de virus o ataques.		
47.2 4	Deberá contar con un tablero ejecutivo de detecciones de malware y de ataques informáticos.		
47.2 5	Deberá contar con un tablero con los usuarios, equipos y ataques más detectados.		
47.2 6	El agente podrá ser actualizado de forma automática desde la consola de administración.		
2. Sistema de detección y repuestas de puntos finales (EDR)			
48	Centralización de la información en la consola central, a fin de conseguir casi un impacto cero en el punto final cuando se realiza un análisis, una investigación o la búsqueda de los elementos involucrados en un ataque.		
49	Deberá crear un árbol de procesos para que en una sola pantalla fácil de leer se indiquen todos los detalles y el contexto del ataque, a fin de realizar investigaciones más rápidas y más sencillas.		



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

50	Interfaz gráfica intuitiva para poder hacer pivotes y ejecutar búsquedas de información referente a los puntos finales en segundos.		
51	Capacidad de contener el punto final o ponerlo en una cuarentena de red tan simple como presionar un botón.		
52	El agente deberá trabajar en modo kernel para poder visualizar y capturar la información para investigaciones forenses		
53	El agente deberá contar un password de protección para desinstalación.		
54	La información de detalles específicos deberá de estar disponible en la consola al menos siete días naturales.		
55	Los detalles de una detección deberán estar disponibles al menos noventa días		
56	Los detalles de una detección deberán contener en caso que aplique al menos lo siguiente:		
57.1	Conexiones de red incluyendo dirección IP origen y puerto utilizado, Dirección IP destino y puerto utilizado		
57.2	Actividades de disco incluyendo carga, lectura, escritura, creación de ejecutables, y eliminación.		
57.3	Indicadores de Inteligencia		
57.4	Consultas DNS realizadas		
57.5	Operaciones de registro de windows realizadas incluyendo creación, modificación y borrado de llaves		
57.6	Actividades y procesos realizados manualmente vía línea de comandos		
57.7	Identificación y/o atribución del ataque identificado a algún grupo de cibercrimen por mecanismos de inteligencia ya sea propia o de terceros, integrada en la solución		
57.8	Deberá de informar todas las conexiones de red realizadas por un host en un tiempo determinado		
57.9	Deberá informar las consultas DNS realizadas por un host en un tiempo determinado		
57.10	Deberá informar los procesos que realizaron modificaciones al firewall de windows en un tiempo determinado		
57.11	Deberá informar la creación de scripts en el punto final en un tiempo determinado		
57.12	Deberá mostrar un gráfico todas las conexiones por escritorio remoto incluyendo usuario y host		
57.13	Deberá mostrar un gráfico todas las conexiones por escritorio remoto incluyendo usuario y host		
57.14	Deberá mostrar un reporte de todos los archivos ejecutados desde la papelera de reciclaje		
58	Deberá incluir una barra de búsqueda para determinar las conexiones realizadas por los puntos finales hacia una lista de dominios, indicando al menos lo siguiente:		

Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

58.1	Cantidad de host que realizaron alguna conexión.		
58.2	Proceso que detonó dicha conexión (process ID)		
58.3	Archivo que realizó la conexión		
58.4	Primer host que realizó la conexión con fecha y hora		
58.5	Ultimo host que realizó la conexión con fecha y hora		
58.6	Usuario registrado en el host que realizó la conexión		
59	Deberá incluir una barra de búsqueda para determinar la lectura y/o ejecución de múltiples indicadores de compromiso en su modalidad hash indicando al menos lo siguiente:		
59.1	Información del archivo ejecutable portable de estar firmado, fabricante, nombre de la aplicación, versión, nombre del archivo y descripción.		
59.2	Historial de carga del archivo en los puntos finales indicando la cantidad de veces y la cantidad de hosts que se haya cargado el módulo		
59.3	Línea de tiempo de los procesos ejecutados		
59.4	Línea de comandos utilizada para la ejecución		
59.5	Primer host que realizó la conexión con fecha y hora		
59.6	Ultimo host que realizó la conexión con fecha y hora		
59.7	Usuario registrado en el host que realizó la conexión		
59.8	Proceso que detonó dicha conexión (process ID)		
60	Notificación inmediata y centralizada sobre ataques masivos de virus y/o código malicioso.		
61	Despliegue de políticas preventivas /reactivas para código malicioso en casos de alerta.		
62	Deberá mostrar un reporte de los nombres de los archivos enviados a dispositivos removibles		
63	Deberá mostrar un reporte de archivos en los puntos finales que coincidan con detecciones de malware por otros fabricantes de antivirus/antimalware que se encuentran en virustotal		
64	Deberá contar con una conexión segura vía powershell a los equipos para realizar respuesta a incidentes, lo anterior si necesidad de permisos adicionales, es decir usando la misma conexión cliente servidor, y con al menos las siguientes funcionalidades: listado de procesos, capacidad de detener procesos (Kill process), dump de procesos, dump de memoria, obtención de muestras, modificación de registros, eliminación de archivos		
65	*		
66	*		
67	*		
68	*		



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

69	*		
70	*		
71	La protección de Firewall deberá mostrar visibilidad instantánea de amenazas potenciales y anomalías de la red.		
72	*		
73	Desinstalación del cliente desde el administrador de programas de Windows o el acceso directo a Uninstall.exe del menú inicio		
74	Desinstalación del cliente de forma remota desde la consola de administración		

Nombre y Firma del Representante Legal (sello)

Para el ítem 2: Se requiere las siguientes especificaciones:

SERVICIOS REQUERIDOS		CUMPLE / NO CUMPLE	# de Pagina
1. Requerimientos técnicos del software			
1	Se requiere que la solución que proponga esté posicionada dentro del cuadrante de "LIDERES" en Gartner 2021 "Magic Quadrant for Endpoint Protection Platforms" Presentar evidencia		
2	El servicio de administración de la solución de protección de servidores deberá contar con una protección coordinada para el firewall, prevención de Intrusiones, antimalware, reputación web, control de aplicaciones, monitoreo de integridad e inspección de bitácoras, usando un único agente instalado en cada máquina virtual (Vmware).		
3	<ul style="list-style-type: none"> • Debe tener compatibilidad con los siguientes sistemas operativos: • Microsoft® Windows®: <ul style="list-style-type: none"> - Windows Server 2019 - Windows Server 2016 - Windows Server 2012 - Windows 10 - Windows 11 • Linux: <ul style="list-style-type: none"> - Red Hat Enterprise Linux 6 (32-bit and 64-bit) - Red Hat Enterprise Linux 7 (32-bit and 64-bit) - CentOS 7 X64 - Oracle Linux 6 X64 - Oracle Linux 7 X64 • VMware <ul style="list-style-type: none"> - VMware vCenter 6.7 with ESXi 6.7 - VMware vCenter 6.5 with ESXi 6.0 or 6.5 - VMware vCenter 6.0 with ESXi 6.0 		
4	La solución deberá administrar desde la misma consola: el firewall, la prevención de Intruso, antimalware, control de aplicaciones, monitoreo de integridad y la inspección de bitácoras.		

Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

5	La consola de administración debe contar con Dashboards que permitan monitorear los equipos de forma sencilla y estos pueden ser personalizados por el administrador		
6	La solución deberá tener la capacidad de reconocer los agentes desplegados en la red a través de una tarea manual o calendarizada.		
7	*		
8	La solución deberá ser capaz de integrarse con Microsoft Active Directory para la administración de usuarios de acceso a la consola y realizar búsqueda de nuevas máquinas en el dominio.		
9	La solución debe contar con políticas por defecto que eviten la desinstalación del agente de seguridad y/o la baja de servicios del mismo. (Agent Self Protection)		
10	La solución debe permitir la creación de políticas globales para todas las maquinas, por perfil e individualmente para cada host		
11	La solución deberá contener un firewall que proteja servidores físicos y/o virtuales administrados desde la misma consola, permitiendo sólo las comunicaciones requeridas entre ellos. Este filtrado debe ser bidireccional y hacerse al menos sobre los siguientes parámetros: *Protocolos: ICMP, IGMP, GGP, TCP, PUP, UDP, IDP, ND, RAW, TCP+UDP *Direcciones MAC *Direcciones IP *Puertos TCP & UDP *Plantillas con reglas predefinidas para plataformas comunes.		
12	*		
13	La solución permitirá monitorear el tráfico para registrar algún ataque y bloquear el tráfico relacionado con él sin afectar el tráfico normal no relacionado con el ataque, permitiendo que continúen disponibles los servicios del servidor.		
14	*		
15	Debe incluir en la integración con los servicios de reputación (del mismo fabricante) para mejorar la protección contra amenazas, incluyendo servicio de reputación de archivo y reputación de URL's		
16	*		
17	Las reglas del firewall debe permitir las siguientes acciones: Allow, Log Only, Bypass, Force Allow y Deny.		
18	La solución deberá ser capaz de bloquear el tráfico de aplicaciones no deseadas como P2P, mensajería instantánea, navegadores web, y muchas otras, definidas por aplicación y no por puerto, de forma tal que otras aplicaciones que usan el o los mismos puertos puedan funcionar de manera normal.		
19	*		



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

20	El módulo de protección del Firewall de host debe contar con la posibilidad de aplicar las políticas de manera programada sobre ciertos horarios.		
21	La solución identifica el software malicioso que accede a la red y reduce la exposición de sus servidores.		
22	*		
23	*		
24	*		
25	La solución deberá ser capaz de detectar y prevenir actividad de conexiones asociadas a ransomware a través de la red, mediante la inspección del tráfico para identificar técnicas de comunicación conocidas utilizadas en ataques de ransomware.		
26	*		
27	*		
28	La solución debe ofrecer la opción de elegir que se ejecute una acción automática en función de la amenaza detectada.		
29	La solución debe contar con la capacidad de limpieza, borrado y envío a cuarentena del archivo detectado como amenaza.		
30	La solución deberá contar con un módulo de protección basado en análisis de comportamiento para protección contra amenazas desconocidas o nuevas variantes, detectando y controlando comportamientos no autorizados u anómalos.		
31	*		
32	*		
33	La solución deberá contar con tecnologías de detección de machine learning para amenazas de día cero.		
34	*		
35	La solución deberá contar con alertas en tiempo real cuando un evento crítico o relevante sea generado, o cuando se detecte una modificación en carpetas, archivos o llaves de registro del sistema operativo y aplicaciones.		
36	La solución debe ofrecer un escaneo que identifique recomendaciones de proceso y servicios que se estén ejecutando para aplicar las reglas de monitoreo.		
37	*		



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

38	La solución debe contar con la capacidad de crear reglas personalizadas para el monitoreo de modificaciones en archivos críticos, carpetas y llaves de registro.		
39	*		
40	*		
41	La solución debe detectar y bloquear software no autorizado automáticamente.		
42	*		
43	*		
44	*		
45	La solución debe permite la generación de reportes bajo demanda o calendarizados permitiendo el envío de dichos reportes vía e-mail, así como generar reporte en formato PDF protegidos con contraseña.		
46	*		
47	*		

Para el ítem 5: Implementación

ITEM	SERVICIOS REQUERIDOS DE IMPLEMENTACION	CUMPLE / NO CUMPLE	# de Pagina
1	Sesión de asesoramiento sobre el diseño de implementación y componentes relacionados a la misma.		
2	Activación de la suscripción - Alta para acceder a la consola de administración y realizar las configuraciones iniciales.		
3	Configuración de las features de los productos solicitados.		
4	Despliegue de veinte (20) agentes en endpoints y servidores.		
5	Gestión y documentación de las configuraciones realizadas. Serán entregables en formato digital (MS Word o PDF).		
6	Se debe incluir traslado de conocimiento de la instalación y configuración de los productos ofertados para que apoye la administración; para un mínimo de tres (3) personas.		
7	Express Support & University LMS Subscription New Customer Access Pass con boucher para examen de CROWDSTRIKE CERTIFIED FALCON ADMINISTRATOR para dos (2) personas.		



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

Para el ítem 6: Soporte local 24 x7 con Ingenieros Certificados

ITEM	REQUERIMIENTOS TÉCNICOS DEL SOPORTE	CUMPLE / NO CUMPLE	# de Pagina
1	El servicio de soporte de la solución ofertada en Item 1, Item 2, Item 3, Item 4 deberá ser disponible 24/7/365 por personal del proveedor y/o del fabricante.		
2	En caso de falla de la solución ofertada. El tiempo máximo para la atención a fallas, será de 4 horas máximo para atención en sitio contado a partir del reporte de la falla a los contactos proporcionados para soporte.		
3	El proveedor deberá brindar entrenamiento para al menos dos (2) personas en el uso de la solución ofertada (no se requiere que entrenamiento sea certificado por el fabricante)		

Nombre y Firma del Representante Legal (sello)



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

FORMATO No. 6 MODELO CARTA DE REFERENCIA LOTE 1

Presentación de al menos tres (3) cartas de referencia con calificación EXCELENTE de empresas a las que haya brindado suministro y configurado las suscripciones del software de seguridad de equipos de la marca ofertada en este proceso en los últimos 5 años (2022,2021,2020,2019, 2018). No se tomarán en cuenta referencias que no sean presentadas en este formato.

San Salvador, (día) de (Mes) de 2022.

Señores:
Banco de Desarrollo de la República de El Salvador
Presente.

Por este medio hacemos constar que la empresa (**Ofertante**) ha suministrado el servicio de: **“Software de Seguridad de equipos Endpoint y Servidores”**, a nuestra empresa/institución, durante el período desde: (**Inicio**) hasta (**Fin**), y ha cumplido con los requerimientos y el tiempo establecido por esta empresa/institución, según detalle siguiente:

No.	CONCEPTO	EXCELENTE	MUY BUENO	REGULAR
1	Cumplimiento de los tiempos de Entrega y Servicio.			
2	Calidad del servicio suministrado.			

Firma Responsable: _____

Nombre Responsable: _____

Cargo: _____

Empresa: _____(Sello)



Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

FORMATO No.7

PERFIL DEL PERSONAL TECNICO ASIGNADO LOTE 1

Detallar al menos tres (3) técnicos certificados en Administración y/o configuración de la marca y software ofertado, al menos dos (2) técnicos de los presentados deberán haber realizado instalación del servicio en un período máximo de 5 años. Incluir la documentación probatoria de las certificaciones y/o cursos tomados por cada uno de los técnicos detallados.

PERFIL TÉCNICO 1				
Nombre				
Formación	Ingeniero	Técnico	Bachiller	Otro
Años de experiencia:				
Certificaciones relacionadas al servicio solicitado:				
Indique al menos un proyecto en las que haya realizado la instalación, configuración y despliegue relacionados al servicio.	Empresa donde se desarrolló el servicio	Mes/Año en que se realizó el servicio	Nombre y contacto de referencia	
Proyecto 1				
Proyecto 2				
Proyecto N				
PERFIL TÉCNICO 2				
Nombre				
Formación	Ingeniero	Técnico	Bachiller	Otro
Años de experiencia:				
Certificaciones relacionadas al servicio solicitado:				
Indique al menos un proyecto en las que haya realizado la instalación, configuración y despliegue relacionados al servicio.	Empresa donde se desarrolló el servicio	Mes/Año en que se realizó el servicio	Nombre y contacto de referencia	
Proyecto 1				
Proyecto 2				
Proyecto N				
PERFIL TÉCNICO N				
Nombre				
Formación	Ingeniero	Técnico	Bachiller	Otro
Años de experiencia:				
Certificaciones relacionadas al servicio solicitado:				
Indique al menos un proyecto en las que haya realizado la instalación, configuración y despliegue relacionados al servicio.	Empresa donde se desarrolló el servicio	Mes/Año en que se realizó el servicio	Nombre y contacto de referencia	
Proyecto 1				
Proyecto 2				
Proyecto N				

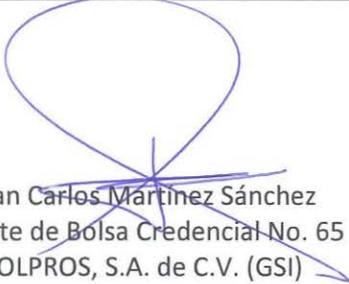
Nombre y Firma del Representante Legal (sello)

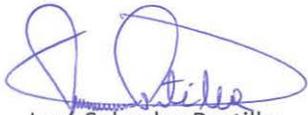


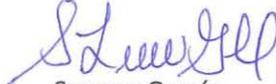
Anexo de Contrato No. 30047, Oferta de Compra No. 372, 28/12/2022

FORMULARIO DE PRECIOS SIN IVA Y CON IVA FORMATO No. 8

Contrato		30047		Número Oferta:		372/2022	
Oferta: PROCESO No. MB-03/2023 "ADQUISICIÓN Y RENOVACIÓN DE LICENCIAMIENTO PARA BANDESAL Y FONDOS QUE ESTE ADMINISTRA"							
ITEM	CANT.	DESCRIPCIÓN	Precio Unitario S/IVA	Monto Total S/IVA	Precio Unitario C/IVA	Monto Total C/IVA	
1	350	CrowdStrike Falcon Endpoint Protection Enterprise. Prevent Insight. Threat Graph Standard. Período de vigencia: 1 de enero al 31 de diciembre de 2023.	\$ 97.47787610619470	\$ 34,117.26	\$ 110.15	\$ 38,552.50	
2	45	CrowdStrike Falcon Server Protection. Server Threat Graph Standard. Período de vigencia: 1 de enero al 31 de diciembre de 2023.	\$ 40.55752212389380	\$ 1,825.09	\$ 45.83	\$ 2,062.35	
3	120	CrowdStrike Falcon Endpoint Protection Pro. Prevent. Período de vigencia: 1 de enero al 31 de diciembre de 2023.	\$ 55.61061946902660	\$ 6,673.27	\$ 62.84	\$ 7,540.80	
4	350	CrowdStrike Falcon Firewall Management. Período de vigencia: 1 de enero al 31 de diciembre de 2023.	\$ 9.66371681415929	\$ 3,382.30	\$ 10.92	\$ 3,822.00	
5	1	Implementación	\$ 9,723.33628318584000	\$ 9,723.34	\$ 10,987.37	\$ 10,987.37	
6	1	Soporte local 24x7 con Ingenieros Certificados en la solución ofertada. Período de vigencia: 1 de enero al 31 de diciembre de 2023.	\$ 3,278.74336283186000	\$ 3,278.74	\$ 3,704.98	\$ 3,704.98	
TOTAL CONTRATO				\$ 59,000.00		\$ 66,670.00	


 Juan Carlos Martínez Sánchez
 Agente de Bolsa Credencial No. 65
 BOLPROS, S.A. de C.V. (GSI)
 Representante del Estado


 José Salvador Portillo
 Agente de Bolsa Credencial No. 62
 Servicios Bursátiles Salvadoreños, S.A de C.V.
 Puesto de Bolsa Vendedor


 Seoany García
 Director de Corro
 BOLPROS, S.A. de C.V.

