GOBIERNO DE EL SALVADOR

CENTRO NACIONAL DE REGISTROS

DOCUMENTO EN VERSIÓN PÚBLICA

De conformidad a los Artículos:

24 letra “c” y 30 de la LAIP.

Se han eliminado los datos personales

BOLPROS
BOLSA DE PRODUCTOS DE EL SALVADOR
Abrimos oportunidades, cerramos tratos.

CONTRATO DE COMPRA VENTA

FECHA:	23 DICIEMBRE DE 2022	**CONTRATO Nº:**	30022
TIPO ENTREGA:	ENTREGA A PLAZOS	**VIGENCIA HASTA:**	31/1/2024
NOMBRE OFERTA:	N° BOLPROS-06/2022-CNR ADQUISICIÓN DE SUSCRIPCIONES DE SOLUCIONES DE SEGURIDAD PARA LA PROTECCIÓN DE ACTIVOS DE INFORMACIÓN INSTITUCIONALES, AÑO 2022"		
PRODUCTO:	SUSCRIPCIÓN DE SOFTWARE DE SEGURIDAD PARA LA PREVENCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIOS (DDOS).		
UNIDAD:	SEGUN ANEXO	**ORIGEN:**	Indiferente
CANTIDAD:	1	**PRECIO UNITARIO US$:**	139500
PLAZO ENTREGA:	SEGUN ANEXO	**PLAZO DE PAGO:**	15 HABILES
GARANTIA FIEL CUMPLIMIENTO:	10.0 %		
PUESTO DE BOLSA O LICENCIATARIO COMPRADOR:	BOLPROS S.A. DE C.V.		
AGENTE DE BOLSA COMPRADOR:			
Nª. CREDENCIAL:			
PUESTO DE BOLSA O LICENCIATARIO VENDEDOR:	SERVICIOS BURSATILES SALVADOREÑOS, S.A. ..		
AGENTE DE BOLSA VENDEDOR:			
Nª. CREDENCIAL:			

DATOS DE LIQUIDACION MONETARIA

VALOR NEGOCIADO:	**US$**	$ 139,500.00
IVA S/VALOR NEGOCIADO:	**US$**	$ 18,135.00
TOTAL:	**US$**	$ 157,635.00

OBSERVACIONES: 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 – 350/2022, 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

FIRMA DEL AGENTE COMPRADOR | FIRMA DEL AGENTE VENDEDOR | FIRMA DEL DIRECTOR DE CORRO

BOLSA DE PRODUCTOS DE EL SALVADOR BOLPROS S.A.

ORIGINAL - BOLPROS

Anexo de Contrato No. 30022, Oferta de Compra No. 350, 23/12/2022

Nombre de oferta	**N° BOLPROS-06/2022-CNR ADQUISICIÓN DE SUSCRIPCIONES DE SOLUCIONES DE SEGURIDAD PARA LA PROTECCIÓN DE ACTIVOS DE INFORMACIÓN INSTITUCIONALES, AÑO 2022"**
Producto	ADQUISICIÓN DE SUSCRIPCIONES DE SOLUCIONES DE SEGURIDAD PARA LA PROTECCIÓN DE ACTIVOS DE INFORMACIÓN INSTITUCIONALES, AÑO 2022
Institución compradora	**CENTRO NACIONAL DE REGISTROS (CNR)**
Precio	**SEGUN ANEXO** **FONDOS PROPIOS**
Cantidad	Ver especificaciones técnicas.
Término	• Bolsa de Productos de El Salvador, Sociedad Anónima de Capital Variable que en lo sucesivo se denominará la Bolsa. • Gerencia de Servicios Institucionales, en lo sucesivo se denominará GSI. • Centro Nacional de Registros, que en lo sucesivo se denominara **CNR.**
Condiciones de Negociación	1. Podrán participar en la presente negociación las personas naturales y/o jurídicas que no se encuentren incapacitadas para ofertar y contratar, impedidas para ofertar y/o inhabilitadas para participar y contratar con la Administración Pública. 2. La negociación se realizará por ítem completo. 3. Cláusula de no colusión: **TRES (3) días hábiles antes de la negociación**, se deberá entregar a BOLPROS, S.A. DE C.V., una Declaración Jurada ante notario en la que manifieste que no ha constituido acuerdos colusorios con uno, varios o todos los demás proveedores que participan en el presente proceso, y que constituyan violación al literal c) del artículo 25 de la ley de competencia según el modelo de declaración jurada establecido en el mecanismo bursátil. Según formato de ANEXO N° 2. 4. Los datos generales del proveedor ANEXO N°. 4, anexado al comprobante de presentación de ofertas técnicas, serán remitidos por el Puesto de Bolsa vendedor a BOLPROS ingresándolos en el sistema de seguimiento de ofertas que la Bolsa ha puesto a disposición; a más tardar el siguiente día hábil después de finalizado el plazo de presentación de ofertas técnicas.
Especificaciones Técnicas	Ver apartado de especificaciones técnicas.
Origen	Indiferente
Fecha, volumen, horario y lugar de entrega	PERIODO DE CONTRATACIÓN Y ENTREGA DE LOS SERVICIOS: Un año a partir de la activación del servicio y la suscripción de la solución, incluye soporte y mantenimiento.

BOLSA DE PRODUCTOS DE EL SALVADOR BOLPROS S.A. de C.V.

Plazo de entrega del documento con la clave de activación desde el sitio web. Será de 7 días hábiles contados a partir del día hábil siguiente de la fecha del cierre del contrato.

LUGAR Y FORMA DE ENTREGA DEL SERVICIO

El lugar de entrega de los servicios será en el Departamento de Seguridad TIC, de la Dirección de Tecnología de la Información del CNR. **La Forma de entrega** es una sola entrega por ítems.

El horario de recepción de los servicios, deberá coordinarse entre el administrador del contrato y la empresa proveedora.

PRÓRROGA EN EL TIEMPO DE ENTREGA DEL SERVICIO

Si durante la ejecución de la entrega del servicio existen demoras por cualquier acto, cambios ordenados en el mismo, inconveniente con el servicio por parte de sus proveedores o cualquier otra causa que no sea imputable al proveedor y que esté debidamente comprobada y documentada, el Proveedor tendrá derecho a que se le conceda una prórroga de acuerdo a la normativa de la Bolsa.

En todo caso, el Proveedor deberá documentar las causas que han generado los retrasos en la ejecución del servicio, las cuales deberán ser confirmadas y autorizadas por el Administrador del Contrato.

La solicitud de prórroga deberá tramitarse de conformidad a lo establecido en la normativa de la Bolsa.

Como otra responsabilidad del Administrador de Contrato, se consignará en este, que dicho administrador, considerando las situaciones imprevistas que sean justificadas técnicamente, podrá designar otro lugar para la entrega del servicio contratado, sin que esto signifique una erogación adicional para el mismo, ni la realización del trámite de modificativa del contrato, el proveedor se obliga a realizar la entrega conforme lo requerido. Para validar este cambio, esta debe ser comunicado a la Bolsa, con la debida anticipación a la fecha estipulada para la entrega, debiéndose realizar toda entrega dentro de la vigencia total del contrato.

VARIACIONES DE LAS CANTIDADES DEL SERVICIO

Ante las necesidades propias de la institución y a solicitud del Administrador del Contrato respectivo y durante la vigencia del mismo, el proveedor deberá estar en la capacidad de aceptar incrementos de los servicios hasta por un TREINTA (30%) del valor contratado aplicando el artículo 83 del Instructivo de Operaciones y Liquidaciones de la Bolsa de Productos de El Salvador, para lo cual se emitirá una Adenda de Incremento y como consecuencia el precio total del contrato podrá variar, tomando siempre como base los precios unitarios de los servicios contratados. A la vez el proveedor deberá entregar la garantía de cumplimiento de contrato correspondiente al monto que se ha incrementado, si es el caso.

Previo al finalizar el plazo del servicio, podrá acordarse con el proveedor una adenda de hasta el 100% del contrato, por un plazo igual o menor, manteniendo las condiciones originales del contrato.

BOLSA DE PRODUCTOS DE EL SALVADOR BOLPROS S.A. de C.V.

Documentación requerida para toda entrega del servicio.	Las entregas deberán acompañarse de la siguiente documentación en original y una fotocopia, la cual deberá ser firmada en la recepción del servicio siempre y cuando se reciban a satisfacción: 1. Orden de entrega del producto emitida por BOLPROS, S.A. DE C.V 2. Nota de envío o Nota de Remisión emitida por el Puesto de Bolsa Vendedor o PROVEEDOR. 3. Fotocopia de contrato emitido por BOLPROS Una vez entregados y recibidos a satisfacción del comprador los documentos detallados anteriormente, el administrador de contrato procederá a emitir la correspondiente acta de recepción.
Garantías	**GARANTÍAS SOLICITADAS:** Los proveedores deberán presentar previo a la negociación: **a) Garantía de Mantenimiento de Oferta** La garantía de mantenimiento de oferta será el **DOS PUNTO CINCO** por ciento **(2.5%) más IVA**, del monto total ofertado. Posterior al cierre de contrato, el proveedor que resulte ganador, deberá presentar: **b) Garantía de Cumplimiento de Contrato** El proveedor para asegurar el cumplimiento de todas sus obligaciones contractuales deberá rendir una garantía de cumplimiento de contrato, equivalente a **DIEZ por ciento (10%) más IVA**, de la suma total contratada, según artículos 7 y 9 del Instructivo de Garantías de la Bolsa de Productos de El Salvador, S.A. de C.V. **Esta garantía se hará efectiva en los siguientes casos:** a) Cuando el proveedor incumpla alguna de las especificaciones consignadas en el contrato sin causa justificada; b) Cuando se comprueben defectos en la entrega del servicio o servicio y el proveedor, sin causa justificada, no subsanare los defectos comprobados en el plazo establecido en el contrato; y, c) En los demás casos establecidos en la Ley y en el Contrato. Las Garantías de Mantenimiento de oferta y de cumplimiento de contrato se deberán emitir a favor de BOLPROS, S.A. de C.V. y serán devueltas una vez se cumpla con las especificaciones del contrato y conforme a la normativa de la bolsa. 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 que puede abreviarse BOLPROS, S.A. de C.V. y serán devueltas una vez se cumpla con los términos del contrato y conforme a la normativa de la bolsa. Las garantías podrán constituirse a través de Fianzas emitidas por afianzadoras, aseguradoras o Bancos autorizados por la Superintendencia del Sistema

<table>
<tr><td></td><td>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 de garantías a nombre de Bolsa de Productos de El Salvador, Sociedad Anónima de Capital Variable, pero debe realizarse con fondos firme, cuenta corriente No. del Banco Cuscatlán.

Si la Garantía es emitida por un Banco Extranjero deberá ser avalada o confirmada por una Institución financiera acreditada en El Salvador.</td></tr>
<tr><td>Penalización económica y Ejecución coactiva</td><td>PENALIZACIÓN ECONÓMICA Y EJECUCIÓN COACTIVA:

PENALIZACIÓN POR ENTREGA EXTEMPORÁNEA

EJECUCIÓN COACTIVA POR PRODUCTOS Y SERVICIO NO ENTREGADOS

El incumplimiento a lo contratado por parte del proveedor será sancionado conforme lo establecido en el Reglamento e Instructivos especiales de BOLPROS, S.A. DE C.V.

En el caso que el proveedor entregue o brinde el servicio fuera del plazo establecido en el Contrato y sus Anexos, junto con la documentación requerida para la entrega, la Institución Compradora podrá permitir la entrega fuera de los plazos establecidos en el contrato, y aplicará una penalización por cada día de extemporaneidad, de acuerdo al detalle siguiente:

<table>
<tr><th>ÍTEMS</th><th>CANTIDAD</th><th>SERVICIO SOLICITADO</th><th>PENALIDAD DIARIA POR ITEMS</th></tr>
<tr><td>1</td><td>1</td><td>SUSCRIPCIÓN DE SOFTWARE DE SEGURIDAD PARA LA PREVENCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIOS (DDOS).</td><td>$125.00</td></tr>
</table>

La penalización mínima a imponer será el equivalente a un salario mínimo del sector comercio.

La penalización deberá ser calculada por la Institución compradora y notificada al proveedor con copia a GSI de BOLPROS.

El cobro de la penalización se realizará dentro de los CINCO (5) días hábiles siguientes a la notificación al proveedor, el cual deberá presentar antes del vencimiento de ese plazo, nota en la cual acepta que se realice el descuento sobre el pago que tenga pendiente, luego el Banco procederá a realizar el descuento de la multa en la factura o Comprobante de Crédito Fiscal CCF, realizando la cancelación de la diferencia después de haber realizado el descuento de penalización.

La Institución Compradora efectuará el cobro de la penalización mediante el descuento bajo figura de compensación cuando efectúe el pago de los productos o bienes.</td></tr>
</table>

	PROCEDIMIENTO PARA LA DETERMINACIÓN DE INCUMPLIMIENTO E IMPOSICIÓN Y CÁLCULO DE PENALIDADES a) Determinación de la penalidad: i- El Administrador de Contrato notificará a la UACI del CNR para que se notifique a la GSI/BOLPROS con nota y documentación de respaldo el plazo incumplido. ii- La Institución Compradora calcula penalización y entrega a Puesto de Bolsa vendedor y éste al Proveedor, la cual será con copia GSI. iii- El Proveedor se presentará a la Tesorería del CNR (UFI), ubicada en Oficinas Centrales, 1ª. Calle Poniente y Final 43 Av. Norte, N° 2310, módulo II, San Salvador, para realizar el pago. b) Procedimiento para el pago de la penalidad: El proveedor deberá presentarse a la Tesorería del CNR (UFI), ubicada en Oficinas Centrales, 1ª. Calle Poniente y Final 43 Av. Norte, N° 2310, módulo II, San Salvador, para realizar el pago. **EJECUCIÓN COACTIVA POR PRODUCTOS Y SERVICIOS NO ENTREGADOS** En caso que los productos no sean entregados, en el plazo original la GSI deberá solicitar a la Bolsa que efectúe la ejecución coactiva del contrato por lo no entregado, de conformidad a los artículos 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. 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 concecido con penalización; conforme a lo dispuesto en los artículos 79 y siguientes del Instructivo de Operaciones y Liquidaciones. Será obligatorio para el Puesto de Bolsa Vendedor e Institución Compradora, 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 negoción en virtud de la ejecución coactiva; caso contrario la Bolsa continuará con el proceso de ejecución hasta la liquidación de la garantía.
Documentación para tramitar cobro y Fecha de pago de anticipos y de productos o servicios	**TRÁMITE DE PAGO** **El método de facturación será directa.** Para trámite de cobro se deberá presentar la siguiente documentación: a) Factura Consumidor Final duplicada del Proveedor a nombre del **Centro Nacional de Registros.** Debiendo incluir el nombre del servicio, número de contrato, el precio unitario y el precio total debe consignarse con dos decimales.

BOLSA DE PRODUCTOS DE EL SALVADOR BOLPROS S.A. de C.V.

Previa notificación por parte del Administrador del Contrato, se emitirá factura de consumidor final, con el detalle de los servicios.

b) En caso de refacturación por errores del proveedor, el tiempo máximo de presentación de las nuevas facturas, no excederá de DIEZ (10) días hábiles y no generará cobro por mora.

c) Acta de recepción del cliente comprador debidamente firmada y sellada por el Administrador de Contrato nombrado para tal efecto.

d) El pago se hará en un plazo máximo de quince (15) días hábiles.

e) De la documentación se presentará original y una fotocopia.

ACTAS DE RECEPCIÓN:

Toda acta de recepción debe ir firmada por el proveedor y Administrador de Contrato nombrado para tal efecto.

Se levantará un acta de recepción debiendo ir firmada por lo menos por el representante del contratista y el Administrador del Contrato nombrado para tal efecto.

Se consignará lugar, día y hora de la recepción, nombre del contratista, firma de la persona que entrega por parte del proveedor, nombre, cargo, referencia del contrato del servicio recibido, detalle, consignación de la conformidad con las especificaciones o características técnicas del servicio requerido, grado de satisfacción, si la entrega se realizó dentro del tiempo establecido, asimismo podrán incluirse observaciones o incumplimientos que a la fecha están en proceso de solventar, detallando en cada informe los tiempos en días hábiles, si existiere mora en la entrega del servicio

Cuando una solicitud de pedido involucre varias entregas parciales, efectuadas siempre dentro del plazo de 10 días hábiles o prorrogados a petición del contratista, los **TRES (3) días hábiles** para entregar actas serán a partir de la última entrega.

Queda definido que la forma de pago por la prestación del servicio será cancelado según la modalidad de pago que sea solicitada por el ofertante, debido a la naturaleza del servicio , con la firma del contrato, la recepción del documento con la clave de activación, la recepción de la factura, la suscripción del acta de recepción recibido a entera satisfacción del CNR firmada y sellada por el Administrador del Contrato y el Representante de la empresa proveedor, para luego ser presentados a tesorería para la emisión del respectivo quedan Contratista.

En cada factura debe reflejarse el **uno por ciento (1%)** en concepto de retención del Impuesto a la Transferencia de Bienes Muebles y la Prestación de Servicios.

De los pagos al proveedor se efectuarán las retenciones establecidas en estos documentos contractuales y de acuerdo a la legislación vigente del país. **La forma de pago será crédito y no contra entrega del referido servicio.**

El trámite de pago se podrá realizar bajo dos modalidades:

BOLSA DE PRODUCTOS DE EL SALVADOR BOLPROS S.A. de C.V.

	a) Pago electrónico con abono a cuenta, para lo cual el proveedor deberá proporcionar un número de cuenta corriente o de ahorros en el cual se le efectuarán los pagos en un banco o cualquier otra institución financiera de las autorizadas y supervisadas por la Superintendencia del Sistema Financiero, donde desean que se le aplique los depósitos, según **ANEXO 6**, el cual deberá ser presentado a la UFI, cuando le sea solicitado. b) Pago se cancele en la Tesorería del CNR, por medio de cheque. Con base en el artículo 82 Bis literal f) de la LACAP, el Administrador del Contrato respectivo remitirá a la UACI en un plazo máximo de **TRES (3) días hábiles** posteriores a la recepción del servicio, el acta respectiva.
Otras Condiciones	1. El contrato se dará por cumplido siempre y cuando el vendedor haya entregado el 100% de lo solicitado. 2. Se aceptan realizar adendas al contrato de acuerdo con los Art. 82 y 83 del Instructivo de Operaciones y Liquidaciones de La Bolsa. 3. Al siguiente día hábil del cierre de la negociación, el Puesto de bolsa vendedor deberá presentar a BOLPROS, S.A. DE C.V., en la GSI los precios de cierre conforme al **ANEXO:7** 4. Los precios unitarios y totales con IVA incluido deben incluir un máximo de 2 decimales.
Vigencia de la suscripción	**Un año contado a partir de la fecha de activación del servicio.**
Vigencia del Contrato	**El plazo de vigencia del contrato es a partir del cierre de negociación hasta el 31 de enero del 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 TÉCNICAS

1. OBJETO DE LA COMPRA

El CNR por medio de la Unidad de Adquisiciones y Contrataciones Institucional (UACI), gestiona el presente proceso por el mecanismo bursátil para la **"ADQUISICIÓN DE SUSCRIPCIONES DE SOLUCIONES DE SEGURIDAD PARA LA PROTECCIÓN DE ACTIVOS DE INFORMACIÓN INSTITUCIONALES, AÑO 2022"**, con la finalidad de contar con soluciones de seguridad para la protección de activos de información institucionales, los cuales se requieren de la siguiente manera:

N° DE ITEM	CANTIDAD	SERVICIO SOLICITADO
1	1	SUSCRIPCIÓN DE SOFTWARE DE SEGURIDAD PARA LA PREVENCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIOS (DDOS).

BOLSA DE PRODUCTOS DE EL SALVADOR BOLPROS S.A. de C.V.

1.1 ESPECIFICACIONES TÉCNICAS

1.1.1 CUMPLIMIENTO TOTAL DE LAS ESPECIFICACIONES TÉCNICAS MÍNIMAS REQUERIDAS PARA CADA UNO DE LOS ÍTEMS: OCHENTA (80) PUNTOS

Cantidad de Licencias: Adquisición de una suscripción de la solución de seguridad para la prevención de ataques de denegación de servicios (DDOS)
Nombre del producto: Solución de seguridad para la prevención de ataques de denegación de servicios (DDOS).
Tipo de Licenciamiento: Suscripción Anual
Idioma: Español
Producto entregable: Documento de adquisición de la suscripción que especifique el servicio que ha sido adquirido por CNR.
Soporte Técnico: Asistencia Técnica 24 horas / 7 días a la semana / 365 días al año. En idioma Español por personal nativo en lenguaje español. Mediante número local. Vía correo electrónico, Web chat y en sitio de ser requerido.
Plazo de entrega: Del documento con la clave de activación desde el sitio web, será de 7 días hábiles contados a partir del día hábil siguiente de la suscripción del contrato. Fecha última de entrega es el 31 de diciembre de 2022.
Período de suscripción y activación: Un año a partir de la activación del servicio y la suscripción de la solución, incluye soporte y mantenimiento.
Contratación: Contratación total de la solución

ÍTEMS N° 1

ESPECIFICACIONES TÉCNICAS PARA LA ADQUISICIÓN DE SUSCRIPCION DE SOLUCIÓN DE SEGURIDAD PARA LA PREVENCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIOS (DDOS)

Los ofertantes deberán detallar en su oferta si cumplen con lo siguiente:

No	FUNCIONES REQUERIDAS EN LA SOLUCIÓN DE SEGURIDAD PARA LA PREVENCIÓN DE ATAQUES DE DENEGACION DE SERVICIOS (DDOS)
	COMPONENTE ONPREMISE
I.	Arquitectura
II.	Capacidad
III.	Funcionalidades de Detección y Mitigación de Ataques
IV.	Consola de Gestión Centralizada
V.	Monitoreo de Seguridad
VI.	Alertas y Reportes
VII.	Servicios de Soporte
	COMPONENTE EN LA NUVE
VIII.	Arquitectura
IX.	Requerimiento de Detección y Mitigación
X.	Arquitectura del Servicio
XI.	Disponibilidad y Niveles de Servicio
XII.	Requerimientos de Portal de Servicios y Visualización
XIII.	Servicio Administrado de Nube DDOS

No	DETALLE DE FUNCIONES REQUERIDAS
	COMPONENTE ONPREMISE
I	**ARQUITECTURA**
1	Cantidad de equipos: 1
2	La solución de mitigación de ataques DDoS se debe integrar a la red de forma transparente en capa 2.
3	Debe soportar despliegues fuera de línea usando puertos SPAN o puertos mirror
4	Cada mitigador de Anti-DDoS debe tener la siguiente configuración de interfaces para su integración a la red. - 6 Interfaces de Cobre con bypass interno - 2 Interfaces de Fibra óptica SFP+. No debe incluir los transceivers.
5	El dispositivo debe incluir al menos dos interfaces de gestión (Management Ports) y administración por consola RJ45.
6	La solución debe soportar bypass por software para pares de puertos individuales.
7	La solución de mitigación de ataques DDoS debe soportar al menos los siguientes tipos de túneles: VLAN Tagging, L2TP, MPLS, GRE, GTP, IPinIP
8	La solución de mitigación de ataques DDoS debe soportar la inspección de los encabezados internos o externos de túneles L2TP, GRE, GTP, IPinIP
9	La solución debe poder monitorear y alertar sobre el uso de CPU de cada política definida de forma independiente.
10	La solución de mitigación de ataques DDoS debe soportar IPv4 e IPv6
11	La solución de mitigación de ataques DDoS debe soportar un número ilimitado de sesiones concurrentes de ataque.
12	La solución de mitigación de ataques DDoS debe incluir doble fuente de poder hot swappable

II	CAPACIDAD
1	La solución de mitigación de ataques DDoS debe estar licenciada para un throughput de tráfico legítimo de al menos 2Gbps
2	La solución de mitigación de ataques DDoS debe soportar crecimiento de throughput por licenciamiento sobre el mismo hardware de hasta 5 Gbps
3	La solución de mitigación de ataques DDoS debe estar licenciada para soportar una capacidad de mitigación mínima de 6 Gbps
4	La solución de mitigación de ataques DDoS debe estar licenciada para soportar una capacidad de mitigación mínima de 7,200,000 PPS por equipo
5	La solución de mitigación de ataques DDoS debe tener una latencia menor a 60 microsegundos.
6	La solución de mitigación de ataques DDoS debe incluir hardware dedicado para la mitigación de ataques SSL/TLS con capacidad de al menos 20K CPS con llaves RSA de 2K.
III	FUNCIONALIDADES DE DETECCIÓN Y MITIGACIÓN DE ATAQUES
1	La solución debe proteger contra al menos las siguientes anomalías de tráfico: - Checksum incorrecto de IPV4. - Tamaño de Cabecera capa invalido. - TTL igual a 0. - Cabecera IPV6 inconsistente. - Limites de salto IPV6 alcanzados. - Protocolo Capa 4 no soportado. - TCP flags invalido. - Tamaño de cabecera UDP invalido. - Dirección de origen o destino igual al Local Host. - Dirección de origen igual a la dirección de destino. - Puerto Capa 4 de origen o destino igual a cero. - Cabera de GRE invalida - Versión GRE Incorrecta
2	La solución debe operar a través de políticas de seguridad con distintas configuraciones de detección y mitigación de acuerdo a los objetos protegidos.
3	Las políticas de seguridad se podrán habilitar o deshabilitar individualmente.
4	Las políticas de seguridad se podrán configurar en modo reporte o en modo bloqueo
5	Las configuraciones de detección y mitigación dentro de una política de seguridad específica, se podrán configurar individualmente en modo reporte o en modo bloqueo
6	La solución debe contar con análisis de comportamiento de red para detectar anomalías de tráfico y prevenir ataques de día cero incluyendo al menos las siguientes inundaciones de tráfico: - Inundación de red UDP. - Inundación de red ICMP. - Inundación de red IGMP. - Inundación de red TCP con flag SYN. - Inundación de red TCP con flag RST. - Inundación de red TCP con flag ACK. - Inundación de red TCP con flag PSH. - Inundación de red TCP con flag FIN. - Inundación de red TCP con flag SYN y ACK. - Inundación de red TCP flag FRAG. - Inundación de red UDP con flag FRAG.
7	La solución debe aprender acerca del tráfico y configurar automáticamente las líneas bases de tráfico y thresholds de ataques.

8	La solución debe permitir crear excepciones de puertos sobre los cuales no se realizará aprendizaje y por ende no se tendrán en cuenta en la creación de las líneas bases.
9	La solución debe correlacionar parámetros que varíen con la tasa de tráfico con parámetros que no varíen con la tasa de tráfico para determinar la condición de ataque.
10	La solución debe incluir un mecanismo preciso de detección de inundaciones UDP que tenga en cuenta parámetros que varíen con la tasa de tráfico y parámetros que no varíen con la tasa de tráfico, incluyendo: - Ancho de banda UDP. - Tasa de paquetes por segundo. - Tasa de conexiones por segundo.
11	La solución debe permitir configurar un umbral de ancho de banda de supresión de aprendizaje, para evitar que las líneas bases se distorsionen en bajo tráfico.
12	La solución debe crear y aplicar automáticamente y en tiempo real una firma para detener los ataques en capa de red.
13	La solución debe proteger contra ataques de tipo ráfaga (burst attacks) identificando que una nueva ráfaga de tráfico pertenece a una firma en tiempo real previamente creada.
14	La solución debe incluir un mecanismo de prevención de overblocking de tráfico el cual valide y refresque la firma, si se está bloqueando más tráfico del debido.
15	La solución debe permitir especificar un límite de tasa de tráfico que servirá como un método alternativo automático a la firma en tiempo real de red.
16	La solución de mitigación de ataques DDoS debe incluir un mecanismo de límite de conexiones TCP y sesiones UDP que cumpla con las siguientes características: - La solución debe contar el número de conexiones TCP o sesiones UDP abiertas por cliente, por servidor, o por la combinación de cliente y servidor. - La solución debe permitir descartar los paquetes que pasen el límite establecido. - La solución debe permitir suspender el tráfico por un tiempo determinado si este pasa del límite establecido.
17	La solución de mitigación de ataques debe incluir un mecanismo que haga seguimiento y bloquee paquetes que superen una tasa de PPS en sesiones definidas.
18	La solución debe incluir protección contra ataques DDoS de inundación de paquetes fuera de estado.
19	La solución debe incluir protección contra ataques DDoS de tipo SYN Flood
20	La protección contra ataques SYN Flood a través del seguimiento de paquetes SYN enviados a cada IP Destino y Puerto.
21	La protección de SYN Flood debe prevenir contra ataques de tipo Spoofed-SYN-flood que vayan dirigidos a múltiples puertos destinos, a través del seguimiento de paquetes SYN enviados a toda la red configurada en la política.
22	La protección de SYN Flood debe contar con al menos dos métodos de autenticación TCP: ACK Fuera de Secuencia y Proxy Transparente
23	La protección de SYN Flood, para los protocolos http y https, debe contar con al menos dos métodos de autenticación: 302 Redirect, Java Script
24	La solución permitirá al operador crear filtros de tráfico.
25	Los filtros de tráfico deben permitir como mínimo seleccionar los siguientes criterios para hacer match al tráfico: -Red de Origen -Red de Destino -Puerto Origen -Puerto Destino -Protocolo -Tamaño del Paquete -Flags TCP -Time to Live (TTL) -Número de Secuencia TCP -Type of Service (ToS) / DSCP

	-Fragment Offset -Fragment ID
26	Los filtros de tráfico deben permitir crear expresiones regulares para filtrar tráfico de acuerdo al payload de los paquetes recibidos.
27	Los filtros de tráfico deben permitir configurar límites de tráfico en PPS o bps, sobre el tráfico que haga match con los criterios definidos.
28	La solución debe contar con protección de ataques DDoS DNS basada en análisis de comportamiento para detectar anomalías de tráfico y prevenir ataques de día cero incluyendo al menos los siguientes tipos de inundaciones de Queries DNS: A, AAAA, MX, PTR, Test, SOA, NAPTR, SRV, Other
29	La solución debe aprender acerca del tráfico DNS y configurar automáticamente las líneas bases de tráfico y thresholds de ataques.
30	La solución debe permitir configurar un umbral de QPS de supresión de aprendizaje, para evitar que las líneas bases se distorsionen en bajo tráfico.
31	La solución debe aprender e incluir en una lista blanca el TOP de FQDNs en el tráfico DNS
32	La lista blanca con el TOP de FQDNs se podrá exportar y se podrán añadir entradas a la lista de forma manual.
33	La solución debe crear y aplicar automáticamente y en tiempo real una firma para detener el ataque de DNS
34	En condición de ataque DDoS, la solución debe bloquear todo el tráfico hacia el DNS que este fuera del complaince del protocolo DNS.
35	La solución debe incluir un mecanismo de reto y respuesta en DNS para minimizar falsos positivos
36	La solución debe mitigar inundaciones de DNS recursivas (inundaciones de dominios aleatorios) bloqueando el tráfico que haga match con la firma en tiempo real creada, mientras permite el tráfico en la lista de FQDNs aprendida.
37	La protección de ataques DDoS DNS de la solución propuesta debe basarse únicamente en el tráfico entrante (Ingress-Only o Inbound).
38	La protección de ataques DDoS DNS debe mitigar ataques de tipo amplificación o reflexión de DNS
39	La protección de ataques DDoS DNS debe mitigar ataques de tipo Brute Force de DNS
40	La solución de mitigación de ataques DDoS debe proteger contra ataques HTTPS Floods
41	La protección contra ataques HTTPS debe soportar las siguientes versiones del protocolo SSL usando hardware dedicado: SSL 3.0, TLS1.0, TLS 1.1, TLS 1.2 y TLS 1.3
42	La protección contra ataques HTTPS debe permitir importar los certificados digitales y asociarlos a los servidores HTTPS protegidos.
43	La protección contra ataques HTTPS debe permitir asignar varios certificados a un objeto protegido y elegir el certificado vía SNI.
44	La protección contra ataques HTTPS Flood debe funcionar a través de análisis de comportamiento del tráfico hacia los servidores HTTPS.
45	La protección contra ataques HTTPS Flood debe aprender y configurar automáticamente las líneas bases y thresholds de ataques sobre cada servidor configurado.
46	La protección contra ataques HTTPS Flood debe correlacionar parámetros que varíen con la tasa de tráfico con parámetros que no varíen para determinar la condición de ataque HTTPS Flood.
47	La solución debe ser capaz de detectar ataques en HTTPS sin necesidad de descifrar el tráfico previamente.
48	La protección contra ataques HTTPS Flood debe funcionar solo con el tráfico de entrante (Ingress-Only o Inbound).
49	La protección contra ataques HTTPS flood debe contar con al menos dos métodos de autenticación: 302 Redirect, Java Script
50	La protección contra ataques HTTPS flood debe identificar automáticamente una lista de IP origen sospechosas del ataque.

51	La protección contra ataques HTTPS Flood debe contar con al menos los siguientes métodos de mitigación: - Mitigación del primer request de los fuentes/orígenes sospechosos haciendo autenticación HTTPS únicamente a las fuentes/orígenes sospechosos - Limitar la tasa de tráfico a los origenes sospechosos - Mitigación del primer request de todos las fuentes/orígenes haciendo autenticación HTTPS a todos los orígenes que se conecten a los servidores protegidos
52	La protección contra ataques HTTPS Flood debe soportar Inspección selectiva completa por cada objeto (servidor) protegido, de tal que forma que el trafico desencriptado después sea pasado por módulos adicionales de mitigación.
53	La protección contra ataques HTTPS Flood podrá anidar distintos métodos de mitigación y dichos métodos escalarán automáticamente en caso de que el ataque no este siendo mitigado.
54	La solución de mitigación de ataques DDoS debe soportar protección Quantile DoS (QDoS) contra micro-inundaciones y pequeños ataques de inundación DoS/DDoS (Phantom floods)
55	La protección Quantile DoS debe soportar los siguientes métodos de mitigación, y deben permitir implementarse de manera escalonada: - Real Time Signature - Top Talkers - Rate Limit
56	La protección Quantile DoS a nivel del método de mitigación "Real Time Signature" debe soportar que: - Cada cuantil utilice un algoritmo de comportamiento para generar una firma en tiempo real - La firma generada se debe basar en el ataque en el cuantil específico - Un perfil de DoS cuantil debe poder contener múltiples firmas (múltiples cuantiles) durante un ataque
57	La protección Quantile DoS a nivel del método de mitigación "Top Talkers" debe bloquear las fuentes (sources)que generan el mayor uso del ancho de banda cuantificado (quantile bandwidth)
58	La protección Quantile DoS a nivel del método de mitigación "Top Talkers" debe soportar el siguiente flujo de mitigación: - Ordenar las fuentes según el tráfico que generan - Comenzar a bloquear las fuentes (sources) una por una, desde la más pesada (heaviest) hasta la más baja, hasta que el tráfico cae por debajo del umbral de ataque
59	La protección Quantile DoS a nivel del método de mitigación "Rate Limit" debe soportar: - Tumbar (drops) el tráfico que supera un determinado umbral - Permitir definir el umbral dependiente de dos parámetros definidos por el usuario: • Sensibilidad de detección (tamaño del cuantil) • Nivel de límite cuantitativo (Rate-Limit)
60	La protección Quantile DoS debe permitir definir los siguientes niveles de sensibilidad de detección: - 0.5% - 1% - 2% - 5% - 10%
61	La protección Quantile DoS debe permitir hacer enforment en las siguientes tasas de cuantil: - Strict (100%) - Moderate (150%) - Permissive (200%)

BOLSA DE PRODUCTOS DE EL SALVADOR BOLPROS S.A. de C.V.

62	La solución debe permitir crear reglas de listas negras y listas blancas, incluyendo al menos los siguientes parámetros de clasificación: - Red Origen - Puerto Origen - Red Destino - Puerto Destino - Protocolo
63	La solución de mitigación de ataques DDoS debe incluir un mecanismo de protección contra escaneos de puertos TCP, UDP e ICMP
64	La protección contra escaneos debe funcionar a través de análisis de comportamiento y el nivel de sensibilidad de la protección debe ser configurado por el operador.
65	La protección contra escaneos debe tener la capacidad de crear listas blancas de direcciones IP origen y puertos
66	La protección contra escaneos debe generar una firma en tiempo real para bloquear el escaneo de puertos realizado.
67	La solución de mitigación de ataques DDoS debe incluir una protección basada en firmas de ataques conocidos que permita al menos mitigar los siguientes tipos de ataques: -Inundaciones TCP, UDPe ICMP conocidas -Herramientas de ataques conocidas disponibles en Internet -Inundaciones de ataques conocidos creados por bots -Vulnerabilidades en los servidores: Web, Mail, FTP, SQL, DNS, SIP -Troyanos y backdoors -Gusanos y Virus -IRC Bots -Spyware -Phishing -Anonymizers
68	La protección basada en firmas de ataques conocidos debe incluir grupos de firmas preconfigurados para ser aplicados en las políticas.
69	La protección basada en firmas de ataques conocidos debe permitir crear grupos de firmas por elementos comunes y aplicar los grupos de firmas en las políticas.
70	La protección basada en firmas debe permitir a los operados crear sus propias firmas.
71	La solución de mitigación de ataques DDoS debe incluir una suscripción para actualización de la protección basada en firmas.
72	La solución de mitigación de ataques DDoS debe incluir una suscripción que permita el bloqueo por geolocalización
73	La protección de geolocalización debe permitir la configuración de un perfil de bloqueo por países y asignarlo a una política de seguridad particular, sin que se afecte el tráfico que haga match con otras políticas.
74	La protección de geolocalización debe permitir la configuración de un perfil para permitir países seleccionados y asignarlo a una política de seguridad particular, sin que se afecte el tráfico que haga match con otras políticas.
75	La solución de mitigación de ataques DDoS debe incluir una lista de IP de mala reputación productos del centro de investigación del fabricante, que será actualizada periódicamente.
76	La lista de IP debe incluir al menos las siguientes categorías: -Atacantes Activos: Direcciones IP que han sido correlacionados y se han determinado como maliciosas. -Tor Exit Nodes: Una IP que es un Tor Exit Node, sin importar si ha participado o no en actividades de ataques. -Web Attackes: Una IP que ha hecho intentos de violaciones Web.
77	Para cada una de las categorías listadas se podrá configurar al menos las siguientes acciones: Bloqueo, Bloqueo y Reporte, Bypass.

78	La lista de IP maliciosas, en conjunto con las acciones configuradas por categorías, debe aplicarse sobre cada política de seguridad.
IV	**CONSOLA DE GESTION CENTRALIZADA**
1	La consola de gestión debe ser del tipo Virtual Appliance y deberá poder instalarse sobre Hyper-V o Vmware ESXI 5 o superior.
2	La consola de gestión debe soportar la administración y monitoreo de todos los Mitigadores que hacen parte de la propuesta
3	La consola de gestión permitirá asignar roles de administración y monitoreo de seguridad por cada uno de los equipos administrados.
4	La consola de gestión debe permitir el acceso a la interfaz gráfica a través del protocolo HTTPS.
5	La consola de gestión debe soporta autenticación remota a través de los protocolos de autenticación RADIUS, LDAP y TACACS+.
6	La consola de gestión debe permitir la configuración de NTP.
7	La consola de gestión deberá permitir el acceso por REST API. Todas las operaciones que puedan realizarse a través de esta API deben estar completamente documentadas.
8	La consola de gestión deberá permitir contar con un repositorio de logs que permitan visualizar todos los cambios de configuración que se realizan sobre los equipos.
9	La consola de gestión debe soportar al menos las siguientes alertas de auditoria y sistema: - Alarmas de servidor. - Alarmas generales del dispositivo (fan, CPU) - Mensajes de auditoría
10	La consola de gestión debe permitir configuración de alertas a servidores de syslog y snmp externos
11	La consola de gestión debe permitir sincronización con un servidor NTP
12	La consola de gestión debe permitir visualizar la utilización de CPU de los dispositivos administrados
13	La consola de gestión debe contar con una funcionalidad que permita la captura de paquetes que ingresan y salen del equipo. Estos archivos deberán estar en formato CAP y deben poder descargarse.
14	La consola de gestión debe permitir definir al menos los siguientes parámetros dentro de la captura: Duración, número de paquetes a Capturar, IP origen, IP Destino, Protocolo
15	La consola de gestión debe permitir creación de tareas calendarizadas de backup de los dispositivos administrados
16	La consola de gestión permitirá guardar los backups localmente o enviarlos a un repositorio externo a través de SCP, SFTP o SSH.
17	La consola de gestión debe permitir creación de tareas calendarizadas para las actualizaciones de seguridad del dispositivo
18	Desde la consola de gestión se podrá realizar la actualización de la versión principal de los dispositivos administrados.
19	Desde la consola de gestión se podrán administrar distintas versiones del dispositivos, teniendo la chance de un rollback de versión en case de necesitarse
20	La consola de gestión debe permitir la administración de múltiples dispositivos, pudiendo realizar configuración simultánea en varios dispositivos.
21	La consola de gestión debe permitir la creación de scripts y flujos de trabajo para automatizar tareas de configuración recurrentes
22	La consola de gestión debe permitir la comparación de la configuración entre dos dispositivos.
23	La consola de gestión debe permitir la comparación de la configuración entre un dispositivo y un backup determinado
V	**MONITOREO DE SEGURIDAD**

1	La consola de gestión debe mostrar en tiempo real los eventos de seguridad detectados por la solución de mitigación de ataques DDoS
2	El monitoreo en tiempo real de los ataques debe mostrar el estado actual de la infraestructura indicando claramente si hay o no un ataque en curso
3	El monitoreo en tiempo real debe mostrar estadísticas gráficas del tráfico total entrante y saliente en bits por segundo y paquetes por segundo
4	El monitoreo en tiempo real debe mostrar estadísticas gráficas de las conexiones por segundo y conexiones concurrentes recibidas.
5	Bajo ataque, el monitoreo en tiempo real debe mostrar por política o objeto protegido al menos la siguiente información: - Tráfico total entrante - Tasa de ataque y tasa de paquetes descartados en bps - Tasa de ataque y tasa de paquetes descartados por cada tipo de mitigación aplicada. - Mitigaciones aplicadas y estadísticas gráficas del ataque que permitan validar el impacto de las contramedidas.
6	El módulo de analítica debe mostrar una gráfica que refleje el estado actual de cada cuantil, según lo definido por el perfil de DoS Quantile, para la política correspondiente.
7	El módulo de analítica de tener un panel de ancho de banda de tráfico, y que sea sólo para la protección DoS Quantile, y este grafico debe mostrar las siguientes curvas: - Recibido - Dropped - Borde de ataque
8	El módulo de analítica de tener un panel de ciclo de vida de la mitigación, y que sea sólo para la Protección DoS Quantile, y este debe mostrar un gráfico con las siguientes curvas: - Firma en tiempo real (RTS). Que permita pasar el cursor sobre una bandera RTS mostrada en la curva del gráfico para ver la firma durante ese tiempo. - Cuántica (Quantile) de los que más hablan - Cuantil Tasa-Límite
9	El módulo de analítica debe permitir tener visibilidad de geolocalización, pudiendo visualizar al menos lo siguiente: - Top de geolocalizaciones atacantes no bloqueadas. - Geolocalizaciones bloqueadas temporalmente. - Geolocalizaciones bloqueadas de forma permanente. - Geolocalizaciones permitidas.
10	Dentro de las funcionalidades de geolocalización, la consola debe permitir el bloqueo temporal de geolocalizaciones seleccionadas.
11	El monitoreo en tiempo real debe mostrar estadísticas gráficas de tráfico por política de seguridad o objeto protegido, para al menos los siguientes tipos de tráficos: SYN, SYN-ACK, RST, FIN-ACK, TCP Fragmented, UDP Fragmented, UDP, ICMP, IGMP
12	El monitoreo en tiempo real debe mostrar estadísticas gráficas de tráfico por política de seguridad o objeto protegido, para al menos los siguientes tipos de queries DNS: Tipo A, AAAA, MX, TXT, SOA, SRV, PTR, NAPTR-
13	El monitoreo en tiempo real debe mostrar estadísticas gráficas de tráfico por cada servidor https protegido
14	El monitoreo en tiempo real debe incluir dashboard con al menos la siguiente información: - Top de Ataques. - Top de Ataques por Ancho de Banda. - Top de los Destinos y Orígenes de los Ataques. - Top de Ataques por Protocolo. - Top de Ataques por Acción de Mitigación.
15	La consola de gestión debe incluir un dashboard en donde se muestre el impacto de las listas de mala reputación configuradas en la solución de mitigación de ataques DDoS.

16	El dashboard de IPs de mala reputación debe incluir el TOP de eventos, TOP de paquetes y TOP por volumen de tráfico, por al menos los siguientes criterios: - Geolocalización - Actividad Maliciosa - Direcciones IP Origen - Línea de tiempo
17	El dashboard de IPs de mala reputación debe permitir modificar el tiempo de muestra datos con una profundidad máxima de 3 meses.
VI	**ALERTAS Y REPORTES**
1	La consola de gestión de permitir generar reportes históricos de los ataques detectados y mitigados por la solución
2	La consola de gestión debe permitir programar tareas de reportes y enviar los reportes vía correo electrónico.
3	La consola de gestión debe permitir configurar un rango de tiempo de hasta 3 meses para la generación de reportes históricos
4	Debe soportar formatos PDF, CSV y HTML para los reportes históricos
5	Debe permitir la personalización del logo de la entidad en los reportes
6	Debe permitir escoger los mitigadores y las políticas de seguridad específicas sobre los cuales se extraerá el reporte.
7	La consola de gestión debe permitir personalizar el contenido de los reportes con mínimo las siguientes estadísticas: - Top de Ataques. - Top de Ataques por Ancho de Banda. - Top de los Destinos y Orígenes de los Ataques. - Top de Ataques por Protocolo. - Top de Ataques por Acción de Mitigación. - Estadística gráfica de ancho de banda. - Tasa de conexión por segundo. - Estadísticas de Conexiones concurrentes.
8	La consola de gestión debe permitir búsquedas de eventos de seguridad a través de la definición de criterios de búsqueda. Como mínimo se deben incluir los siguientes criterios: - Duración del Ataque. - Ancho de banda del Ataque. - Cantidad de paquetes por segundo. - Dirección IP Origen o Dirección IP Destino. - Categoría del Ataque.
9	La consola de gestión debe permitir anidar múltiples criterios a través de expresiones regulares
10	Desde la consola de gestión se deben enviar alertas de ataques
11	Debe permitir escoger los mitigadores y las políticas de seguridad específicas sobre los cuales se realizará la configuración de la alerta
12	Desde la consola de gestión se podrá personalizar el tipo de alertas que se enviarán a través de la creación de expresiones regulares con al menos los siguientes criterios: - Riesgo del Ataque. - Duración del Ataque. - Ancho de banda del Ataque. - Cantidad de paquetes por segundo. - Categoría del Ataque.
13	Desde la consola de gestión se podrá configurar la severidad de la alerta
VII	**SERVICIOS DE SOPORTE**
1	El soporte técnico deberá ser ofrecido directamente por el fabricante de la solución durante el periodo de 1 año. El canal debe realizar el nivel 1 de soporte.

2	Se deberá prestar el soporte de fábrica con SLA de 7x24x365 durante la vigencia del contrato.
3	Se deberá incluir RMA para reemplazo de partes con SLA NBD Shipment desde fábrica.
4	El oferente deberá entregar un manual con el procedimiento de apertura de casos de soporte con el fabricante.
	COMPONENTE EN LA NUBE
VIII	**ARQUITECTURA**
1	El servicio se debe bridar en modalidad Hibrido bajo demanda en donde todo el tráfico es enrutado hacia un dispositivo mitigador en cada premisa y en caso de ataque volumétrico, el tráfico deberá desviarse hacia la nube de Cloud DDoS para máxima protección y granularidad, por un periodo de suscripción de 1 año.
2	El servicio debe dimensionarse teniendo en cuenta un ancho de banda de tráfico legítimo de 500 Mbps
3	El servicio debe incluir un número de ilimitado ataques por mes, con una duración por ataque de ilimitadas horas.
4	El servicio debe incluir protección de los siguientes activos: 6 segmentos BGP /24 o 30 direcciones IP (DNS)
5	La capacidad total mínima del servicio de Cloud DDoS debe ser de 10Tbps
6	La tecnología ofertada en la premisa debe ser la misma tecnología usada para la detección y mitigación en la nube, de tal forma que permita la sincronización de las estadísticas de tráfico, la información de ataque, las líneas base y políticas flotantes creadas.
IX	**REQUERIMIENTO DE DETECCIÓN Y MITIGACIÓN**
1	El servicio debe contar con al menos las siguientes técnicas de detección: - Detección a través de Análisis de Comportamiento. - Detección a través de la Correlación de parámetros rate variant y rate invariant. - Detección a través de la tasa de tráfico. - Detección por anomalías de tráfico. - Detección por firmas de patrones de ataques conocidos. - Detección automática de ataques a través del mitigador DDoS CPE instalado en la premisa.
2	El servicio debe contar con al menos las siguientes técnicas de Mitigación: - Mitigación a través del descarte de paquetes que hagan match con anomalías - Mitigación a través del descarte de paquetes que hagan match con firmas de ataques conocidos - Mitigación a través de la creación de una contramedida en tiempo real para bloquear ataques de día cero - Mitigación a través de retos y respuesta en TCP para evitar falsos positivos - Mitigación a través de retos y respuesta en HTTP para evitar falsos positivos - Mitigación de ataques HTTP/S Floods - Mitigación de ataques DNS Floods combinando modelos de seguridad positivos y negativos - Mitigación a través de listas negras
	El servicio debe contar con la siguiente cobertura mínima de ataques: - UDP Floods - SYN Floods - TCP Floods - ICMP Floods - IGMP Floods - TCP out of state floods (RST y ACK Floods) - DDoS Volumétricos: Reflection, Amplification - SSL Negotiation Floods - HTTPS Floods - HTTP page flood attacks - DNS Floods Attacks

BOLSA DE PRODUCTOS DE EL SALVADOR BOLPROS S.A. de C.V.

	- SIP Floods Attacks - Ataques DDoS lanzados con herramientas conocidas
X	**ARQUITECTURA DEL SERVICIO**
1	El servicio debe contar con métodos de desvío de tráfico estándar, BGP y DNS, en caso de ser necesario.
2	En caso de utilizar BGP, se debe configurar inyección de tráfico vía GRE, en caso de ser necesario.
3	El servicio debe contar con la opción de configurar los desvíos de tráfico de forma manual, en caso de ser necesario.
4	El servicio debe contar con la opción de configurar los desvíos de tráfico de forma automática independiente del método de desvío, BGP o DNS, en caso de ser necesario.
5	Debe contar con la opción de configurar sesiones BGP sobre túneles GRE para influenciar el tráfico y configurar desvíos automáticos, en caso de ser necesario.
6	El servicio debe incluir una opción de desvío o cancelación del desvío a través de un botón en el portal de servicio o vía API.
7	El servicio soporta alertas en tiempo real a través del al menos los siguientes medios: Portal, SMS, e-mail y API.
8	El servicio debe contar con al menos 16 centros de limpieza distribuidos alrededor del mundo.
9	Los centros de limpieza del servicio alrededor del mundo deben estar conectados en full-mesh usando enrutamiento basado en Anycast
XI	**DISPONIBILIDAD Y NIVELES DE SERVICIO**
1	El servicio debe tener una disponibilidad de 99.999% medida anual
2	El servicio debe contar con un SLA de detección inmediata de ataques
3	El servicio debe contar con un SLA de notificación de 2 minutos vía el portal de servicios o a través de API
4	El servicio debe contar con un SLA de notificación de 15 minutos vía llamada telefónica/SMS/E-mail.
5	El servicio debe garantizar un SLA de desvío de tráfico de 1 minuto para desvío automático, en caso de ser necesario.
6	El servicio debe garantizar un SLA de desvío de tráfico de 15 minutos para desvío manual, en caso de ser necesario.
7	El servicio debe garantizar un SLA de desvío de tráfico de 1 minuto una vez se active el desvío vía API o desde el portal, en caso de ser necesario.
8	El servicio debe garantizar un SLA de desvío de tráfico de 1 minuto para configuración de BGP sobre GRE, en caso de ser necesario.
9	El servicio debe garantizar un SLA de mitigación de ataques de red: UDP/ICMP Flood, SYN Floods, TCP Flag Abuses Attacks en segundos.
10	El servicio debe garantizar un SLA de mitigación de ataques de aplicación GET/POST Floods en segundos.
11	El servicio debe garantizar un SLA de mitigación de ataques de aplicación DNS Floods en segundos.
12	El servicio debe garantizar una consistencia en la mitigación del 95%.

BOLPROS S.A. de C.V. BOLSA DE PRODUCTOS DE EL SALVADOR

XII	REQUERIMIENTOS DE PORTAL DE SERVICIOS Y VISUALIZACIÓN
1	El servicio debe incluir un portal para administración y visualización del servicio.
2	El portal debe permitir auto gestión de los usuarios.
3	El acceso al portal debe contar con doble factor de autenticación.
4	El acceso al portal debe poder restringirse por las direcciones IP origen de los operadores.
5	Desde el portal se debe configurar el tipo de alertas, por severidad, a recibir por usuario.
6	El servicio debe proveer envío de alertas de seguridad en: Portal, vía e-mail y vía SMS.
7	El servicio debe proveer envío de alertas operacionales en: Portal, vía e-mail y vía SMS.
8	El portal debe proveer los detalles de la cuenta del cliente.
9	Desde los detalles de la cuenta se debe configurar los detalles redirección: Ancho de Banda Crítico y Duración Crítica de un Ataque.
10	El portal debe mostrar todos los assets protegidos.
11	El portal debe entregar un resumen de los servicios adquiridos: Fecha de Suscripción, Ancho de banda y Assets.
12	El servicio debe proveer un portal Web con múltiples cuentas de administración y permita personalización de vistas.
13	El servicio debe contar con estadísticas del tráfico en bps y pps para el tráfico entrante al Scrubbing center
14	El servicio debe contar con estadísticas del tráfico en bps y pps para el tráfico limpio.
15	El servicio debe contar con estadísticas del tráfico en bps y pps para el tráfico entrante del mitigador de Anti-DDoS en la premisa.
16	El servicio debe contar con estadísticas del tráfico en bps y pps para el tráfico limpio que sale del mitigador de Anti-DDoS ubicado en premisas.
17	El servicio debe mostrar gráficos con el TOP de los vectores de ataque
18	El servicio debe mostrar gráficos con el TOP de las IP Origen
19	El servicio debe mostrar gráficos con el TOP de las IP Destino
20	El portal debe advertir acerca del estado del servicio, es decir, si los assets protegidos están o no bajo ataque.
21	El portal debe advertir acerca del estado de la redirección, es decir, si los assets protegidos se encuentran o no en la nube.
22	La información en el portal debe retenerse por al menos 3 meses, pudiendo filtrar la información mostrada por diferentes rangos de tiempo.
XIII	**SERVICIO ADMINISTRADO DE NUBE DDOS**
1	El servicio de Cloud DDoS debe tener una cobertura de soporte 7x24x365.
2	El servicio debe contar con la posibilidad de apertura de casos vía telefónica, o a través de portal de soporte.
3	Debe contar con un servicio de respuesta a emergencias, con un máximo 30 minutos de tiempo de respuesta.
4	El servicio debe proveer asistencia bajo demanda para la mitigación de ataques DDoS.
5	Debe contar con asistencia durante el proceso de onboarding.
6	El servicio debe monitorear el estado de salud de lo(s) mitigador(es) en la premisa.
7	El servicio contará con alertas proactivas y automáticas de seguridad y anomalías.
8	El servicio debe contar con Reportes de seguridad periódicos configurados desde el portal

2. JUSTIFICACIÓN DE LA UNIDAD SOLICITANTE

1.1 SUSCRIPCIÓN DE SOFTWARE DE SEGURIDAD PARA LA PREVENCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIOS (DDOS). Los ataques de red distribuidos a menudo se conocen como ataques de denegación distribuida de servicio (DDOS). Este tipo de ataque aprovecha los límites de capacidad específicos que se aplican a cualquier recurso de red, tal como la infraestructura que habilita el sitio web de la empresa. El ataque DDOS envía varias solicitudes al recurso web atacado, con la intención de desbordar la capacidad del sitio web para administrar varias solicitudes o saturar el enlace de acceso por internet, lo que se traduce en una afectación en la disponibilidad del servicio. Con base en el crecimiento de ataques de denegación de servicios conocidos a nivel nacional y en la región, y en el impacto que éste podría tener a nivel institucional en caso de materializarse, se requiere la contratación de una solución de seguridad que implemente la protección contrata ataques por agotamiento de recurso y ataques de tipo volumétrico, orientados a provocar la suspensión temporal de servicios institucionales disponibles al público.

1.2 SUSCRIPCIÓN DE SOFTWARE DE SEGURIDAD PARA LA PROTECCIÓN DE LA BASE DE DATOS INSTITUCIONAL.

Las bases de datos están expuestas a diferentes tipos de ataques cibernéticos que aprovechan múltiples vulnerabilidades asociadas al motor de base de datos, acceso de usuarios, ejecución de comandos de forma no autorizada, exfiltración de información, cifrado de datos, entre otros. En atención a ello, se requiere la adquisición de una herramienta de seguridad que permita mantener una gestión adecuada de accesos, uso de privilegios, monitoreo sobre transacciones realizadas, control de exfiltración de información, ataques por ransomware, bloqueo de transacciones indebidas y visibilidad de riesgos para prevenir violaciones de datos y automatización de respuesta ante incidentes.

2.3 SOLUCIÓN DE SEGURIDAD PARA LA GESTIÓN DE ACCESOS CON PRIVILEGIOS.

En el entorno empresarial, el acceso con privilegios es un término que se utiliza para designar el acceso o las capacidades especiales por encima de las de un usuario estándar. Los usuarios privilegiados necesitan acceso a cuentas privilegiadas para realizar rutinas diarias como el mantenimiento de los sistemas, la actualización y la resolución de problemas. Sin embargo, estos usuarios también pueden hacer un mal uso de los privilegios para obtener acceso no autorizado a la información y causar daños al entorno de TI. La Gestión de Acceso Privilegiado, es una estrategia integral de ciberseguridad (que comprende personas, procesos y tecnología) para controlar, supervisar, proteger y auditar todas las identidades y actividades con privilegios humanas y no humanas en todo el entorno informático de una empresa, para evitar el mal uso de los privilegios por parte de los usuarios autorizados y para detectar actividades maliciosas que podrían indicar una cuenta de usuario comprometida, se requiere la adquisición de una solución que permita realizar la gestión de acceso privilegiados que registre y supervise todas las actividades de las sesiones con privilegios.

BOLSA DE PRODUCTOS DE EL SALVADOR BOLPROS S.A. de C.V.

2.4 SUSCRIPCIÓN DE SOFTWARE DE SEGURIDAD PARA EL PARCHEO VIRTUAL PARA SERVIDORES INSTITUCIONALES.

La obsolescencia de los sistemas operativos de servidores implica que una vez que se cumple la fecha de fin de soporte declarada por el fabricante éste deja de generar parches de seguridad para la mitigación de vulnerabilidades, esto representa un riesgo importante ya que a pesar que el sistema operativo ha sido declarado obsoleto, muchas veces por múltiples razones la migración hacia un sistema operativo que tenga soporte del fabricante no es inmediato, esta situación expone a las instituciones a ataques que aprovechen dichas vulnerabilidades debido a la ausencia de parches de seguridad. Para superar esta situación se requiere la implementación de una solución que permita implementar parches de seguridad virtuales en servidores legados, mitigando el riesgo sin afectar el funcionamiento del sistema operativo.

2.5 FIREWALL PARA APLICACIONES WEB (WAF).

En la actualidad, los servicios en línea representan para la institución una de las principales estrategias para la atención de solicitudes de la ciudadanía, ya que permiten atender en formato 24/7/365, los ataques cibernéticos basados en aplicaciones web representan el principal vector para las instituciones con aplicaciones expuestos a internet, la seguridad de las aplicaciones web requiere de una variedad de procesos, tecnologías y métodos para proteger los servidores web, las aplicaciones web y los servicios web, de las amenazas que suponen los ataques basados en internet. La seguridad de las aplicaciones web es fundamental para proteger los datos, los clientes, las organizaciones del robo de datos, las interrupciones en la continuidad de negocios u otras consecuencias perjudiciales del delito cibernético, por esta razón se requiere la contratación de una solución de seguridad que permita mitigar el riesgo de ataques por medio de aplicaciones web externas, protegiendo de múltiples ataques a los servidores de aplicaciones, garantizando la integridad, confidencialidad y disponibilidad de la información.

3. MARCO LEGAL

El presente proceso estará sujeto a la Constitución de la República, Ley de Adquisiciones y Contrataciones de la Administración Pública (LACAP) artículo 2 letra e), normativa BOLPROS y demás normativas vigentes aplicables.

4. ACEPTACIÓN Y PREPARACIÓN DE OFERTAS

El proveedor al presentar su oferta, acepta sin reservas las especificaciones técnicas, condiciones, indicaciones y términos establecidos, los cuales constituyen el marco normativo que regirá el procedimiento de adquisición y contratación, así como la formulación y ejecución del contrato.

Para preparar su oferta, el proveedor deberá examinar cuidadosamente lo detallado en cada una de las secciones e incluyendo los anexos del presente documento.

Este sufragará todos los costos relacionados con la preparación y presentación de su oferta. Será responsable por las consecuencias y costos provenientes de la falta de conocimiento o errónea interpretación de este documento.

5. IDIOMA DE LA OFERTA

Las ofertas, así como toda la correspondencia y documentos relativos a ella, que intercambien el proveedor y el CNR, deberán redactarse en idioma castellano, o traducirse a dicho idioma.

Los documentos complementarios y literatura impresa que proporcione el proveedor podrán estar escritos en otro idioma, a condición que vaya acompañado de una traducción fiel del documento en idioma castellano.

Los documentos públicos que sean extendidos por Instituciones o autoridades extranjeras, deben presentarse debidamente apostillados, según el Convenio de la Haya o legalizada por el correspondiente consulado de conformidad al artículo 334 del Código Procesal Civil y Mercantil, según el caso.

6. IMPEDIDOS PARA OFERTAR Y CONTRATAR

Podrán ofertar y contratar con la administración pública, todas las personas naturales o jurídicas, nacionales o extranjeras, que tengan capacidad legal para obligarse; conforme al derecho común y las jurídicas legalmente constituidas, con facultades legales, técnicas y financieras para proporcionar el servicio requerido, incluyendo a la micro, pequeña y mediana empresa, siempre que estas puedan garantizar la calidad y demás condiciones del servicio requerido.
Si alguno de los Ofertantes, a la fecha de presentación de ofertas, así como durante el período de evaluación de ofertas se encontrare en el registro de inhabilitados e incapacitados de la UNAC, publicado en COMPRASAL, automáticamente quedará descalificado y no será sujeto de negociación, lo cual será verificado de oficio por el CNR y comunicada por está a Bolpros.
El proveedor deberá declarar que no se encuentra incapacitado para ofertar y contratar, así como sobre otras condiciones establecidas en el **Anexo 1 Declaración Jurada**.

7. RESPONSABILIDAD SOCIAL PARA LA PREVENCIÓN Y ERRADICACIÓN DEL TRABAJO INFANTIL

En caso se comprobaré por la Dirección General de Inspección de Trabajo del Ministerio de Trabajo y Previsión Social, incumplimiento por parte del oferente a la Normativa que prohíbe el trabajo infantil y de Protección de la persona adolescente trabajadora; se iniciará el procedimiento para determinar el cometimiento o no dentro del procedimiento adquisitivo, o durante a la ejecución contractual. En caso se comprobare por la Dirección General de Inspección de Trabajo y Previsión Social, incumplimiento por parte del proveedor a la normativa anterior, la institución compradora iniciará el procedimiento de ejecución coactiva por incumplimiento a obligaciones contractuales, de conformidad al **Anexo 1 Declaración Jurada**.

8. CRITERIOS DE EVALUACIÓN DE OFERTAS

La oferta técnica deberá ser presentada de conformidad a las especificaciones establecidas en la Oferta de Compra, debiendo además incorporar los documentos de respaldo que se le solicite.

Las ofertas serán evaluadas por la unidad solicitante del CNR, a efecto de verificar el contenido, documentación y cumplimiento conforme lo solicitado en la Oferta de Compra, legislación vigente aplicable, así como la correspondencia tramitada en el proceso de elaboración y evaluación de ofertas, utilizando para ello los factores y criterios de evaluación establecidos en la Oferta de compra. Posteriormente a la evaluación

respectiva se dará a conocer las ofertas que han cumplido lo solicitado para seguir en el proceso de la negociación.

Para que las ofertas puedan ser evaluadas, se verificará cumplimiento de requisitos como se detalla a continuación:

PARÁMETRO		CONDICIÓN		EVALUADOR
		MÁXIMO	MÍNIMO	
Evaluación Técnica	**Primera etapa** Condiciones a cumplir de carácter obligatorio	Condiciones a cumplir de carácter obligatorio		Unidad Solicitante
	Segunda etapa Criterios técnicos ponderados	100 puntos	90 puntos	

9. SUBSANACIÓN DE ERRORES U OMISIONES EN LA OFERTA

Durante el proceso de evaluación, la compradora por medio de la UACI a través de la Bolsa, **PODRÁ PREVENIR:**

1. Errores u omisiones de alguna documentación que no haya sido incluida en la Oferta Técnica, o que siendo incluida tenga algún error u omisión.
2. Así como también podrá hacer consultas al proveedor con el objeto de aclarar dudas sobre las especificaciones técnicas u otros aspectos de lo ofertado, siempre que se encuentren considerados como situaciones subsanables y que no modifiquen el contenido de la Oferta de Compra.

   Se le otorgará al proveedor un plazo improrrogable y perentorio como máximo de hasta **TRES (3) días hábiles**, contados a partir del día siguiente de la notificación, para que conteste por escrito la prevención, aclare lo solicitado, remita los documentos requeridos, corrija el error o cumpla con la omisión detectada. Si dentro del plazo otorgado no subsanare la prevención o la respuesta, o no aclara lo solicitado en la Evaluación Técnica, se asignará cero puntos al parámetro de evaluación que dio lugar a dicha solicitud y se evaluará con la información disponible al momento.

10. EVALUACIÓN DE LA OFERTA TÉCNICA

Los proveedores deben mencionar en sus documentos de oferta, su disposición a cumplir con cada uno de los requerimientos e ítems mencionados en la **Sección III de "Especificaciones Técnicas"**, así como toda la documentación detallada en este numeral, presentando además la **CARTA COMPROMISO** según **anexo 5.**

PRIMERA ETAPA

CONDICIONES A CUMPLIR DE CARÁCTER OBLIGATORIO:

La oferta que no cumpla con las condiciones de carácter obligatorio, **habiéndoseles**

prevenido, no continuarán con el proceso de evaluación técnica, según verificación de la documentación solicitada, de acuerdo al siguiente detalle:

N°	OTROS REQUISITOS A CUMPLIR	CUMPLE	NO CUMPLE
1	**PROVEEDOR DISTRIBUIDOR** Presentar carta vigente del fabricante, firmada por el(los) fabricante(s) o de su representante o del representante regional para Latinoamérica o Centroamérica en original o fotocopia simple o cuenta de correo electrónico para corroborar la veracidad y validez en la cual establezca que el Oferente es distribuidor autorizado en El Salvador para comercializar la solución requerida.		
2	**PROVEEDOR REDISTRIBUIDOR** En el caso que el Oferente sea un re-distribuidor, debe presentar además del documento anteriormente requerido para el distribuidor lo siguiente: Presentar carta vigente en original o fotocopia simple: en este último caso agregar cuenta de correo electrónico para corroborar la veracidad y validez en la cual establezca que el oferente es redistribuidor autorizado en El Salvador para comercializar la solución requerida.		
	ASPECTOS GENERALES		
	La empresa debe contar con personal certificado en la solución (presentar documentación de al menos dos personas certificadas en la solución). Deberán adjuntar los atestados y presentarlos en copia simple: curriculum, certificaciones u otra documentación que le acredite.		
	La empresa deberá indicar en su oferta que entregará garantía de soporte técnico y mantenimiento no menor a doce meses, mediante certificado de garantía o carta del contratista, la cual deberá ser presentada al administrador del contrato al momento de firmar el acta de recepción.		
	CONFIDENCIALIDAD. El o la Contratista se compromete a firmar un acuerdo de confidencialidad sobre la información sensible que sea revelada por el Contratante, independientemente del medio empleado para transmitirla, ya sea en forma verbal o escrita, y se compromete a no revelar dicha información a terceras personas, salvo que el Contratante lo autorice en forma escrita.		

SEGUNDA ETAPA

Una vez verificado el cumplimiento de las condiciones de carácter obligatorio, se tomará en cuenta los criterios a evaluar para dicho servicio, de acuerdo a las especificaciones técnicas de cada uno de ellos y con base a las ponderaciones establecidas en dicha sección:

BOLSA DE PRODUCTOS DE EL SALVADOR BOLPROS S.A. de C.V.

Anexo de Contrato No. 30022, Oferta de Compra No. 350, 23/12/2022

N°	DESCRIPCIÓN		PUNTAJE
1	**CUMPLIMIENTO TOTAL DE LAS ESPECIFICACIONES TÉCNICAS MÍNIMAS REQUERIDAS** Los proveedores deberán presentar las especificaciones técnicas del fabricante por ítem completo, proporcionando la información que sirva para evaluar y comprobar el servicio ofertado tales como: brochures o fotos legibles, y/ o manuales de uso según aplique, identificándolos con su número de ítems, cantidad y descripción del servicio con sus Especificaciones técnicas detalladas y claras.		80
	Falta de cumplimiento de una o más de las especificaciones técnicas		0
2	**EXPERIENCIA DEL PROVEEDOR** El proveedor deberá presentar **TRES (3) cartas o constancias** de referencia originales o fotocopias simples, emitidas en fecha posterior a la publicación de la oferta de compra del sitio web de BOLPROS, dirigidas al CNR o a quien interese, por instituciones públicas y/o privadas, refiriéndose a servicios similares a los solicitados dentro de los últimos **TRES (3)** años, e indicando los requisitos siguientes: ✓ Nombre del proveedor. ✓ Descripción del servicio. ✓ Período de contrato u Orden de Compra ✓ Cantidad del servicio contratado ✓ Si el servicio ha sido recibido a entera satisfacción debiendo ser excelente o muy bueno. ✓ Si cumplieron con los tiempos de entrega del servicio, calidad de los productos contratados y atención oportuna a los problemas. Las cartas o constancias para su validez deberán presentarse firmadas y selladas por el respectivo Titular, o Autoridad o Director o Gerente o Encargado de la Administración del Contrato u órdenes de compra de la Institución, indicando teléfono, correo electrónico y nombre de la persona de contacto, dicha información podrá ser verificado por el CNR, con las instituciones emisoras. Las cartas de referencias podrán ser presentadas de acuerdo al **Anexo 4,** de no haber sido extendidas de acuerdo a éste formato, deberán contener los requisitos anteriormente solicitados. Se aceptarán cartas o constancias de referencia emitidas por una misma Institución o empresa siempre y cuando sea de contratos u órdenes de compra en diferentes contratos y se le asignará la ponderación correspondiente. Dicha información podrá ser corroborada por el CNR con las entidades emisoras, en caso de presentar fotocopias simples.		20
	Presenta 3 cartas o constancias de experiencia en el servicio o presenta 1 carta o constancia emitida por una misma entidad en la que se haga constar la experiencia de	20	

N°	DESCRIPCIÓN		PUNTAJE
	3 contrataciones dentro de los últimos 3 años y cumplen en su contenido con lo solicitado.		
	b) Presenta 2 cartas o constancias de experiencia en el servicio o presenta 1 carta o constancia emitida por una misma entidad en la que se haga constar la experiencia por dos contratos dentro de los 3 últimos 3 años y cumplen en su contenido con lo solicitado.	10	
	c) Presenta 1 carta o constancia de experiencia en el servicio y cumplen en su contenido con lo solicitado	5	
	d) No presenta carta de experiencia en el servicio	0	
TOTAL			100

Debido a que la negociación y cierre del contrato podrá ser **POR ÍTEM COMPLETO COMPLETO,** independientemente de cualquiera de los ítems o lotes, las especificaciones técnicas se revisarán de forma individual por cada ítem y lote, de acuerdo a las especificaciones técnicas de cada uno de ellos y los proveedores continuarán en el proceso de evaluación técnica únicamente con aquellos ítems que hubieren cumplido.

Se evaluará la documentación presentada en la Oferta Técnica, verificando los parámetros de evaluación antes relacionados, estableciéndose un puntaje mínimo de **NOVENTA (90) PUNTOS** para que el o los ítems completos sean considerados **ELEGIBLES** para continuar con la negociación; los parámetros de experiencia serán evaluados solamente una vez y su resultado se mantendrá constante para la evaluación individual de cada ítem.

11. CRITERIOS PARA LA CONTRATACIÓN

Una vez desarrollado todo el proceso de evaluación de ofertas presentadas, se determina la oferta que cumple con los requisitos establecidos en las Especificaciones Técnicas. Se considerarán para efectos de negociación y cierre de contrato los criterios siguientes:

a) El CNR se reserva el derecho de contratar el servicio objeto de este proceso en forma **TOTAL** o **PARCIAL POR ÍTEM COMPLETO,** así como **declararla desierta o sin efecto**.

b) Las ofertas que no cumplan los requerimientos mínimos solicitados en las presentes Especificaciones Técnicas, no serán objeto de negociación en la BOLSA.

c) El CNR podrá negociar el servicio hasta donde lo permita la disponibilidad presupuestaria.

d) Con base al principio de racionalidad del gasto público, el CNR podrá no negociar el servicio, cuyos precios no estén acordes a los precios del mercado.

e) El CNR se reserva el derecho de reducir las cantidades del servicio de acuerdo a la disponibilidad financiera, sin ninguna variación en las demás especificaciones y condiciones de la oferta, y existieren razones presupuestarias para ello, sin que el proveedor pueda modificar sus precios unitarios ofertados.

f) Los proveedores que estuviesen sancionados con multas por incumplimientos contractuales con el CNR, deberán estar solvente en el pago de las mismas al momento de formalizar nuevos contrato.

BOLSA DE PRODUCTOS DE EL SALVADOR BOLPROS S.A. de C.V.

g) Si alguno de los proveedores, a la fecha de presentación de ofertas, así como durante el período de evaluación de ofertas se encontrare en el registro de inhabilitados e incapacitados de la UNAC, publicado en COMPRASAL, automáticamente quedará descalificado y no será sujeto de negociación, lo cual será verificado de oficio por el CNR y comunicada por ésta a Bolpros.

12. PROHIBICIÓN

El proveedor no podrá ceder, traspasar o subcontratar a ningún título los derechos y obligaciones que emanen del contrato. Ningún subcontrato o traspaso de derecho, relevará el proveedor, ni a su fiador de las responsabilidades adquiridas en el contrato y en las garantías.

13. OBLIGACIONES ESPECIALES DEL PROVEEDOR

Además de las obligaciones enunciadas en el resto de los numerales de las Especificaciones Técnicas, se detallan las siguientes obligaciones que tienen un carácter especial:

a) El proveedor contratista deberá cumplir con la legislación aplicable, Oferta de Compra y con las instrucciones que le giren la Institución Administradora del Contrato.

b) Atender con prioridad los requerimientos del CNR.

c) Garantizar y mantener la calidad de los servicios que entregue.

d) El proveedor deberá entregar el servicio en óptimas condiciones, garantizando el buen funcionamiento soporte y mantenimiento para el CNR.

e) Atender el llamado que se le haga por medio del Administrador de Contrato respectivo, para resolver cualquier petición relacionada con el servicio contratado.

f) La solución de seguridad objeto del servicio, será revisado minuciosamente, por parte del Administrador de Contrato respectivo.

g) Se aclara que los servicios deberán ser entregados y cobrados en el presente año fiscal.

14. RECLAMACIÓN DE DAÑOS, PERJUICIOS Y VICIOS OCULTOS

El plazo para que se extinga la responsabilidad al proveedor por daños, perjuicios y vicios ocultos prescribirá en el plazo establecido en los artículos 2253 y siguientes del Código Civil.

15. RECLAMACIÓN POR VICIOS Y DEFICIENCIAS

Si se observare algún vicio o deficiencia en el servicio proporcionado por el proveedor, el CNR por medio de la persona nombrada como Administrador del Contrato respectivo, podrá reclamar al proveedor por escrito y pedirá la subsanación que dio lugar a dicho falta, vicio o deficiencia, dentro de un plazo de **DIEZ (10)** días hábiles posteriores a la fecha de notificación del reclamo por parte del Administrador del Contrato respectivo, pudiendo este reprogramar dicho plazo en casos justificados.

El mecanismo a utilizar se podrá gestionar inicialmente por medio de llamadas telefónicas, correo electrónico, fax o contacto directo o por medio de correspondencia escrita.

Identificado y documentado la falta por el Administrador de Contrato respectivo, éste deberá proceder a realizar el reclamos oportunamente y por escrito el proveedor quien deberá resolver en forma y tiempo establecido en el reclamo.

El Administrador del Contrato respectivo informará por escrito a la UACI cuando el proveedor no solvente satisfactoriamente el reclamo realizado en el tiempo establecido, adjuntando documentos que comprueben el cumplimiento, así como la respuesta que el proveedor ha manifestado, para iniciar el procedimiento administrativo sancionador establecido en la normativa de la Bolsa.

16. SOLUCIÓN DE CONTROVERSIAS Y ARBITRAJE

Se seguirá de acuerdo a **Normativa de BOLPROS.**

BOLSA DE PRODUCTOS DE EL SALVADOR BOLPROS S.A. de C.V.

ANEXO 6

DECLARACIÓN JURADA DE AUTORIZACIÓN DE DEPÓSITOS DE PAGO PARA PROVEEDORES Y PROVEEDORS DEL CNR

1.0 DECLARANTE

1.1 PERSONA NATURAL O JURÍDICA			
NOMBRE Y APELLIDO O RAZÓN SOCIAL	NIT	DUI O PASAPORTE	TELÉFONO
DIRECCIÓN	CIUDAD	CORREO ELECTRÓNICO	
1.2 REPRESENTANTE LEGAL O APODERADO (SOLO PERSONAS JURÍDICAS)			
NOMBRES Y APELLIDOS	NIT	CORREO ELECTRÓNICO	TELÉFONO

Por este medio declaro bajo juramento que las cuentas que detallo a continuación, serán utilizadas por el CENTRO NACIONAL DE REGISTROS, para cancelar cualquier obligación legalmente exigible, según lo establecido en el artículo 77 de la Ley Orgánica de Administración Financiera del Estado.

La cuenta a declarar es la siguiente:

NOMBRE DE LA CUENTA	NÚMERO DE CUENTA	CORRIENTE	AHORRO	NOMBRE DE LA INSTITUCIÓN FINANCIERA

DECLARO BAJO JURAMENTO LO SIGUIENTE.

1. Que los datos que proporciono en este documento son verdaderos y que conozco las Normas Legales y Administrativas que regulan esta declaración jurada.
2. Que en caso de actuar como representante legal, declaro que el poder con el que actúo es suficiente para asumir todas las responsabilidades.

San Salvador, ___ de ___ de 20___.

FIRMA
NOMBRE
DUI

BOLSA DE PRODUCTOS DE EL SALVADOR BOLPROS S.A. de C.V.

Anexo de Contrato No. 30022, Oferta de Compra No. 350, 23/12/2022

FORMULARIO DE PRECIOS SIN IVA Y CON IVA

ANEXO 7

Contrato	30022		Número Oferta:	350/2022		
Oferta:	N° BOLPROS-06/2022-CNR ADQUISICIÓN DE SUSCRIPCIONES DE SOLUCIONES DE SEGURIDAD PARA LA PROTECCIÓN DE ACTIVOS DE INFORMACIÓN INSTITUCIONALES, AÑO 2022"					
N° DE ÍTEMS	SERVICIO OFERTADO	CANTIDAD	Precio Unitario S/IVA	Monto Total S/IVA	Precio Unitario C/IVA	Monto Total C/IVA
1	SUSCRIPCIÓN DE SOFTWARE DE SEGURIDAD PARA LA PREVENCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIOS (DDOS).	1	$ 139,500.00	$ 139,500.00	$ 157,635.00	$ 157,635.00
TOTAL CONTRATO				$ 139,500.00		$ 157,635.00

BOLPROS, S.A. de C.V. (GSI)
Representante del Estado

Servicios Bursátiles Salvadoreños, S.A de C.V.
Puesto de Bolsa Vendedor

BOLPROS, S.A. de C.V.

BOLSA DE PRODUCTOS DE EL SALVADOR, BOLPROS S.A. de C.V.