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:**	30021
TIPO ENTREGA:	ENTREGA A PLAZOS	**VIGENCIA HASTA:**	31/1/2024
NOMBRE OFERTA:	Nº BOLPROS-06/2022-CNR ADQUISICIÓN DE SUSCRIPCIONES DE SOLUCIONES DE SEGURIDAD PARA LA PROTECCIÓN DE ACTIVOS DE INFORMACIÓN INSTITUCIONALES, AÑO 2022"		
PRODUCTO:	ITEMS: 2, 3, 5,		
UNIDAD:	SEGUN ANEXO	**ORIGEN:**	Indiferente
CANTIDAD:	SEGUN ANEXO	**PRECIO UNITARIO US$:**	SEGUN ANEXO
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:			
Nº. CREDENCIAL:			
PUESTO DE BOLSA O LICENCIATARIO VENDEDOR:	SERVICIOS BURSATILES SALVADOREÑOS, S.A. ..		
AGENTE DE BOLSA VENDEDOR:			
Nº. CREDENCIAL:			

DATOS DE LIQUIDACION MONETARIA

VALOR NEGOCIADO:	**US$**	$ 206,800.00
IVA S/VALOR NEGOCIADO:	**US$**	$ 26,884.00
TOTAL:	**US$**	$ 233,684.00

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. de C.V.

Anexo de Contrato No. 30021, 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.

Anexo de Contrato No. 30021, Oferta de Compra No. 350, 23/12/2022

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

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

	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.
Penalización económica y Ejecución coactiva	**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:

ÍTEMS	CANTIDAD	SERVICIO SOLICITADO	PENALIDAD DIARIA POR ITEMS
2	1	SUSCRIPCIÓN DE SOFTWARE DE SEGURIDAD PARA LA PROTECCIÓN DE LA BASE DE DATOS INSTITUCIONAL.	$145.00
3	1	SOLUCIÓN DE SEGURIDAD PARA LA GESTIÓN DE ACCESOS CON PRIVILEGIOS.	$28.00
5	1	FIREWALL PARA APLICACIONES WEB (WAF).	$15.00

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.

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

	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. **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 concedido 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.

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:** 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:

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

N° DE ITEM	CANTIDAD	SERVICIO SOLICITADO
2	1	SUSCRIPCIÓN DE SOFTWARE DE SEGURIDAD PARA LA PROTECCIÓN DE LA BASE DE DATOS INSTITUCIONAL.
3	1	SOLUCIÓN DE SEGURIDAD PARA LA GESTIÓN DE ACCESOS CON PRIVILEGIOS.
5	1	FIREWALL PARA APLICACIONES WEB (WAF).

1.1 ESPECIFICACIONES TÉCNICAS

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

ÍTEMS N° 2

FUNCIONES A REALIZAR POR LA SOLUCIÓN DE SEGURIDAD PARA LA PROTECCIÓN DE LA BASE DE DATOS INSTITUCIONAL

Los ofertantes deberán detallar en su oferta si la solución cumple con las funciones siguientes:

ESPECIFICACIONES TECNICAS PARA LA ADQUISICIÓN DE SUSCRIPCION DE SOLUCIÓN DE SEGURIDAD PARA LA PROTECCIÓN DE LA BASE DE DATOS INSTITUCIONAL
Cantidad de Licencias: Adquisición de suscripción de solución de seguridad para la protección de la base de datos institucional.
Nombre del producto: Solución de seguridad para la protección de la base de datos institucional.
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.
Período de suscripción y activación: Un año a partir de la activación del servicio y la suscripción de la solución, incluye soporte y mantenimiento

o	FUNCIONES REQUERIDAS EN LA SOLUCIÓN DE SEGURIDAD PARA LA PROTECCIÓN DE LA BASE DE DATOS INSTITUCIONAL
	Condiciones Generales
	Administración
	Análisis de vulnerabilidades
	Bloqueo
	Control de permisos de usuarios
	Descubrimiento
	Despliegue
	Integración
	Monitoreo
	Seguridad
	Perfilamiento
	Analítica
	Retención
	Licenciamiento
	Del proveedor

N°	DETALLE DE FUNCIONES REQUERIDAS
	Condiciones generales
1	La solución Database Activity Monitoring (DAM) / DBF (Database Firewall) debe tener la capacidad de capturar todas las acciones de usuario relacionadas con las bases de datos. Estas acciones se deben capturar sin requerir mecanismos propios-nativos de las bases de datos. Los motores que debe soportar la solución deben ser por lo menos los siguientes:
	- MariaDB Server
	- Microsoft SQL Server
	- MySQL
	- Oracle
	- PostgreSQL
2	La solución debe contar con el correspondiente respaldo del fabricante, para los servicios de garantía de hardware (si aplica), mantenimiento software y soporte técnico
3	El fabricante de la solución deberá contar con un centro de investigación que se encargue de generar mecanismos de detección de ataques hacia las Bases de Datos y de cumplimiento de estándares de seguridad y auditoría de la industria; estos mecanismos podrán ser firmas, políticas, vulnerabilidades, plantillas, entre otros. Dicho contenido deberá ser descargable de forma periódica por la solución para incrementar su capacidad de detección, mitigación de amenazas y cumplimiento.
	Administración
4	La solución deberá ser administrada desde una sola consola (centralizada) WEB que permita la gestión de las políticas (auditoría y seguridad), informes, reportes, revisión de auditoría, monitoreo, eventos de seguridad, gestión de los distintos componentes de la solución y el monitoreo de su estado y rendimiento.
5	La solución deberá permitir realizar respaldos periódicos en forma automática de toda la información almacenada en el mismo, incluyendo las configuraciones de todos los módulos administrados y tener la capacidad de transferirlos automáticamente a un servidor remoto utilizando los protocolos SCP y FTP. El respaldo deberá estar cifrado. La periodicidad de los respaldos se debe poder establecer desde la consola de administración
6	Toda la configuración, administración y monitoreo de la solución se efectuará a través de la consola de administración
7	La solución de administración debe permitir asignación de perfiles de administración por usuarios y estos perfiles deben permitir separar roles de administración y monitoreo.

8	Deberá permitir la definición de roles de usuarios de forma granular, de tal forma que un rol tenga acceso a determinadas vistas o menús de la solución
9	Deberá proporcionar una vista centralizada de los logs, entendiendo como tal, la unificación de los logs de la totalidad de los componentes que conforman la solución.
10	La solución deberá realizar detección y análisis sobre todo el tráfico en tiempo real, sin necesidad de crear un archivo log primero para su análisis posterior.
11	La solución de administración permitirá, como mínimo, lo siguiente:
	- Agregar, eliminar o modificar la configuración en un entorno gráfico
	- Modificar las reglas de los diferentes equipos
	- Efectuar la configuración de los componentes de la solución
	- Visualizar los registros de auditoria, alertas de seguridad y eventos del sistema.
	- Generar reportes ajustables por el usuario
12	Permitir la generación de reportes, de toda la actividad registrada en los logs, en los formatos PDF y CSV
13	Permitir la elección de información a ser incluida en los reportes de forma granular, con la capacidad de elegir las columnas a mostrar en los reportes y filtrar la información a ser mostrada. Asimismo, podrá generar diagramas ejecutivos de barra o pastel en los reportes PDF.
14	Capacidad de automatizar la generación de reportes y su posterior remisión por correo electrónico
	Análisis de vulnerabilidades
15	La solución deberá poder realizar escaneos a las bases de datos en diferentes niveles/capas, según lo siguiente:
	- Brindar un puntaje de los riesgos e indicar cómo mitigar esos riesgos
	- Escaneo de vulnerabilidades de la base de datos y configuraciones erróneas, como contraseñas predeterminadas.
	- Escaneo de cumplimiento de estándares de benchmarks o hardening como CIS y DISA-STIG
16	El análisis de vulnerabilidades no debe requerir la instalación de software en el servidor de la base de datos
17	La solución deberá contar con un dashboard que permita comparar una tarea de escaneo de vulnerabilidades actual con uno anterior, para verificar si las vulnerabilidades o configuraciones erróneas han sido solucionadas
	Bloqueo
18	La funcionalidad de Bloqueo deberá estar activa en el mismo equipo que realiza el monitoreo de actividad de la base de datos (DAM)
19	La solución deberá realizar bloqueos de ataques y actividades no autorizadas hacia las bases de datos en tiempo real
20	De acuerdo con la detección de ataque debe permitir tomar diferentes acciones:
	- Bloqueo de comando SQL
	- Bloqueo de la dirección IP correspondiente a la petición, durante una cantidad de tiempo definible.
21	La funcionalidad de Bloqueo no deberá depender de la funcionalidad de Auditoría, es decir, se podrá implementar una política de Bloqueo para determinada transacción SQL, independientemente si dicha transacción SQL tiene una política de Auditoría asociada.
	Control de permisos de usuarios
22	Deberá contar con la funcionalidad de (mediante escaneos) poder realizar informes sobre:
	- Permisos efectivos de los usuarios sobre los distintos objetos de las bases de datos

	- Detección de usuarios "Dormant" o en desuso y cuáles de ellos están o no bloqueados
	- Cadenas de autorización que permiten que cierto usuario (a través de ciertos roles) tenga un permiso específico
	- Relacionar un permiso otorgado a cierto usuario con quién lo otorgó (Grantee).
Descubrimiento	
23	La solución deberá realizar descubrimientos automatizados (escaneos) en la red para identificar servidores de base de datos ya sea a nivel de servicio o puertos habilitados
24	La solución deberá tener la capacidad de descubrir y clasificar información sensible dentro de las tablas de bases de datos de acuerdo con las políticas de negocio. Las definiciones de que se considera información sensible deberán poder crearse de manera flexible y granular. Deberá contar de forma preconfigurada con patrones de detección de datos sensibles acorde a regulaciones como GDPR
Despliegue	
25	La solución deberá soportar implementar los appliances en modo "Inline Bridge" para auditar todo tipo de transacción SQL y/o bloquear a nivel de la red antes de que los querys SQL lleguen a los servidores; despliegues en modo Sniffing conectado a un puerto espejo (port mirror) de un dispositivo de red o utilización de TAPs de red; utilización de agentes en los servidores de bases de datos a nivel de sistema operativo (sin modificar ningún binario de los motores), debe contar con capacidad de auditar y bloquear transacciones SQL en base a políticas determinadas
Integración	
26	La solución debe soportar el protocolo de gestión de red SNMP para ser monitoreados por las herramientas de terceros
27	El sistema debe permitir la integración y envío de alertas a terceros u herramientas de correlación (SIEM) a través de syslog
Monitoreo	
28	La solución deberá incluir agentes livianos de software para monitoreo de actividad sobre el servidor, sin depender de auditoría nativa de las bases de datos o logs propios de los motores de base de datos. Asimismo, la solución no deberá depender únicamente de dichos agentes para poder protegerlos y/o monitorearlos
29	Los agentes deberán poder desactivarse si superan determinado umbral del consumo de CPU del servidor donde se encuentra instalado. Asimismo, para mejorar el rendimiento, el agente podrá contar con políticas que permitan excluir determinados eventos (incluyendo procesos confiables del servidor de Base de Datos y/o eventos originados a partir de una IP determinada).
30	Los agentes deberá ser compatibles con Sistemas Operativos basado en Linux
31	Deberá registrar todas las pistas de auditoría de manera detallada de todas las actividades referentes a las bases de datos, que permita conocer por cada transacción "quién, qué, dónde, cuándo y cómo".
32	La solución, para efectos de obtener los registros de auditoría de las transacciones de Base de Datos no deberá requerir ningún cambio en la configuración o contenido de la base de datos. Esto incluye:
	- Creación de usuarios en las bases de datos.
	- Modificación de los permisos de los usuarios existentes.
33	La solución deberá implementar un monitoreo efectivo de usuarios privilegiados (DBA, super usuarios, desarrolladores, etc.).
34	La solución deberá monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL
35	La solución deberá monitorear tanto el tráfico local y el remoto de las bases de datos

36	La solución deberá ofrecer la posibilidad de auditar las sesiones de base de datos. La auditoría debe incluir los siguientes datos:
	- Fecha y hora de la ocurrencia del evento.
	- Información de usuario de base de datos.
	- Información de los objetos de bases de datos (tablas, vistas, vistas materializadas, store procedures, entre otros) consultados/modificado y los datos consultados (resultados de la consulta).
	- Instancia, esquema, base de datos, objeto y operación realizada
	- Debe mostrar las variables bind en caso que éstas sean utilizadas por la aplicación
37	La solución deberá manejar funcionalidades tan amplias o granulares como se requieran, que deberán poder ser construidas manualmente. Los criterios deberán poder usarse varios a la vez y en diferentes combinaciones de ellos:
	- Tipo de datos accedido
	- Acceso a datos marcados como sensibles
	- Base de Datos, Schema, Instancia, Tabla y Columna accedido
	- Estado de autenticación de la sesión
	- Usuario y/o Grupo de Usuarios de Base de Datos conectado
	- Logins, Logouts, Queries
	- IPs de origen y destino
	- Nombre de Host origen
	- Aplicación usada para la conexión a la base de datos
	- Tiempo de respuesta/procesamiento del query
	- Número de ocurrencias en intervalos de tiempo definidos
	- Por operaciones básicas (Select, Insert, Update, Delete)
	- Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Restore)
	- Por Stored Procedure o Function utilizada
	- Hora del Día
38	La solución deberá soportar la importación de certificados en formato PKCS12 y PEM
39	La solución deberá tener capacidad de monitorear el tráfico encriptado hacia las Bases de Datos (local y remoto), esto incluye Oracle ASO y MSSQL con Diffie Helfman
40	Por cada política de auditoría se podrá especificar una cuota de espacio en disco para almacenamiento de eventos, de tal forma que las políticas consideradas críticas puedan tener mayor espacio de almacenamiento que otras políticas no críticas
41	Por cada política de auditoría se podrá determinar si los logs de transacciones SQL serán respaldados en un servidor externo (FTP o SCP), indicando una frecuencia de respaldo automático.
42	Por cada política de auditoría se podrá definir si la solución también tendrá la capacidad de almacenar los logs de respuesta de la Base de Datos al hacer una consulta a una tabla (SELECT)
43	La solución debe poder integrarse a una SAN para poder expandir su capacidad de almacenamiento
44	La solución deberá tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema, entre otras; hacia otras herramientas de administración por medio de protocolos SNMP y SYSLOG.
	Seguridad
45	La solución deberá proveer detalles sobre alertas generadas y deberá tener la facilidad de modificar las políticas asociadas desde las alertas
46	Deberá poder restringir una petición de base dependiendo de:

	- Usuarios de bases de datos, Usuarios de Sistema operativo, IP y nombre de host de origen, binario o programa utilizado para conectarse
	- Base de datos, tabla, stored procedure, esquema
	- Tablas, esquemas, columnas
	- Operaciones realizadas (DELETE, UPDATE, GRANT, ALTER, etc.)
	- Horarios de ejecución de operaciones
	- Cantidad de registros devueltos en un query y tiempo de respuesta
47	La solución deberá detectar anomalías y abusos a los protocolos de red, malformaciones en los protocolos SQL y firmas de ataque conocidas destinadas a los servidores protegidos.
48	Deberá soportar el modelo negativo de seguridad, el cual define explícitamente las firmas de ataques conocidos, por lo que deberá además cumplir con las siguientes especificaciones:
	- Deberá bloquear las transacciones que tengan contenido que coincida con firmas de ataque conocidos.
	- Deberá incluir una lista preconfigurada y detallada de las firmas de ataque.
	- Deberá permitir la modificación o adición de firmas por el administrador.
	- Deberá permitir la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes.
	- Deberá detectar o prevenir amenazas conocidas en múltiples niveles, incluyendo, la red, sistemas operativos, software del servidor web y ataques a nivel de aplicación.
49	La solución debe detectar los siguientes eventos de seguridad:
	- Acceso de usuario desconocido
	- Acceso de aplicación de base de datos desconocida
	- Acceso de cliente (origen IP) desconocido
	- Intento de ejecución de inyección de comandos SQL
	- Ejecución de un Stored Procedure desconocido
	- Acceso a una base de datos y o esquema no autorizado
	- Acceso a bases de datos, esquemas o tablas previamente definidas
	- Ejecución de comandos privilegiados (DDL).
	- Ejecución de comandos SQL no autorizados.
50	La solución deberá examinar y correlacionar eventos que individualmente podrían no constituir un riesgo pero que en conjunto son ataques complejos intentando vulnerar las aplicaciones.
	Perfilamiento
51	La solución deberá contar con tecnología de autoaprendizaje con mínima intervención humana. El proceso deberá ser constante y deberá aprender la estructura de las bases de datos, incluyendo bases de datos, tablas, aplicaciones, IP origen, querys, así como el comportamiento de cada usuario; todo esto para el establecimiento de una línea base de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.
	Analítica
52	La solución debe contar con un mecanismo de inteligencia artificial que detecte usuarios comprometidos cuyas credenciales son robadas o que, sin saberlo, introducen malware en la empresa
53	La solución debe contar con un mecanismo de inteligencia artificial que detecte Usuarios malintencionados que deliberadamente roban o manipulan activos institucionales
54	La solución debe contar con un mecanismo de inteligencia artificial que detecte Usuarios descuidados que inadvertidamente ponen en riesgo datos confidenciales
55	La solución debe contar con un mecanismo de inteligencia artificial que aprenda dinámicamente los patrones normales de acceso a los datos de los usuarios y luego identifique la actividad de acceso inapropiada o abusiva para alertar de manera proactiva a los equipos de TI sobre comportamientos peligrosos

56	El mecanismo de analítica debe tener la capacidad de agregar patrones de comportamiento en listas blancas, por tiempos determinados para que no se emitan alertas o se generen incidentes que coincidan por el periodo establecido
57	El mecanismo de analítica debe tener la capacidad de dar visibilidad ante al menos para los siguientes eventos:
	- Modificaciones a las auditorías nativas con la intención de eliminar rastro de actividades maliciosas
	- Intento de ejecución de comandos de sistema operativo aprovechando alguna vulnerabilidad en la base de datos
	- Intento de robo de credenciales de las bases de datos consultando la metadata de las mismas
	- Exfiltración de datos
	- Modificación de la configuración o inclusión de elementos dentro de la base de datos que permitan vulnerar/atacar la información
	- Inclusión de código binario (malware) en los motores de bases de datos con el objetivo de atacar o correr código arbitrario con funciones diferentes a las autorizadas
	- Ataques que aprovechando vulnerabilidades de las bases de datos hayan logrado o hayan intentado leer archivos propios del sistema operativo
	- Un usuario malintencionado ataca la base de datos e intenta explotar una vulnerabilidad o una característica de la base de datos para obtener privilegios elevados sobre recursos y / o datos
	- Un usuario malintencionado ataca la base de datos y realiza una secuencia sospechosa que se identifica como una campaña de ransomware
	- Se utiliza una cuenta para acceder a la base de datos en un momento atípico para un usuario y su grupo de pares
	- Un usuario interactivo (humano) está utilizando una cuenta de servicio para acceder a la base de datos
	- Una persona consulta registros en exceso de lo que normalmente consulta el, su grupo de pares y la organización
	- Un usuario no ha podido iniciar sesión satisfactoriamente más veces de lo habitual para este propietario de cuenta en particular
	- Un usuario no pudo iniciar sesión (satisfactoriamente) en la base de datos desde un servidor de aplicaciones
	- Un usuario ha intentado acceder a una cantidad anormalmente alta de bases de datos diferentes durante un corto período de tiempo
	- Un usuario inició sesión en el dispositivo corporativo de otro empleado para acceder a una base de datos
	- Un usuario interactivo (humano) accede directamente a datos comerciales a los que normalmente solo se debe acceder a través de una aplicación
	- Un usuario realizó un comando que es de naturaleza altamente sospechosa y se ejecutó de una manera anormal
	- Un usuario interactivo (humano) ha consultado una base de datos utilizando consultas SQL dinámicas de forma anormal
	- Un usuario interactivo (humano) ha escaneado tablas sensibles del sistema en varias bases de datos durante un período de tiempo relativamente corto de forma anormal
Retención	
58	La solución debe permitir almacenar por lo menos un año de eventos de auditoría, los cuales deben poder ser consultados en línea, es decir, sin requerir importar al sistema archivos externos como backups u otro mecanismo que implique realizar una operación que no sea inmediata y/o algún procedimiento manual
Licenciamiento	

59	La solución debe manejarse bajo un esquema de licenciamiento por suscripción, la cual debe ser renovada cada año.
60	La solución debe de contar con un mínimo para cuatro servidores de base de datos y en caso de requerir más pueda permitir añadir licencias extras por servidor de base de datos, una vez se utilice el licenciamiento base contratado en la suscripción el cual debe incluir 4 servidores de base de datos
61	La solución debe permitir añadir el número necesario de appliances virtuales DBF, sin costo alguno, para cumplir con la transaccionalidad necesaria, en base al número de servidores de bases de datos que se tengan licenciados.
	Del Proveedor
62	La empresa que oferte deberá de mostrar por medio de una carta del fabricante que tiene autorización de vender su herramienta
63	La empresa que oferte deberá de contar por lo menos con 4 personas certificadas en la solución
64	La empresa que oferte deberá de contar por lo menos con más de 10 años de experiencia en la venta de Seguridad de la Información
65	La empresa que oferte deberá de contar con dos personas certificada en ISO 27001, Esto con el objetivo de guiar las mejores prácticas de seguridad a la hora de la implementación

ESPECIFICACIONES TECNICAS PARA LA ADQUISICIÓN DE SUSCRIPCION DE SOLUCIÓN DE SEGURIDA PARA A GESTIÓN DE ACCESOS CON PRIVILEGIOS Los ofertantes deberá detallar en su oferta si cumplen con lo siguiente:
Cantidad de Licencias: Adquisición de una suscripción de la solución de seguridad para la Gestión de Accesos con Privilegios
Nombre del producto: Solución de seguridad para la Gestión de Accesos con Privilegios.
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.
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

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

ÍTEMS N° 3

SOLUCIÓN DE SEGURIDAD PARA GESTIÓN DE ACCESOS CON PRIVILEGIOS

FUNCIONES A REALIZAR POR LA SOLUCIÓN DE SEGURIDAD PARA LA GESTIÓN DE ACCESOS CON PRIVILEGIOS

No	FUNCIONES REQUERIDAS EN LA SOLUCIÓN DE SEGURIDAD PARA LA GESTIÓN DE ACCESOS CON PRIVILEGIOS
	Condiciones generales
	Arquitectura de la solución y sistema de respaldo
	Administración de la solución
	Gestión de contraseñas
	Rotación de contraseñas
	Control de acceso
	Integraciones y compatibilidad
	Registro de activos
	Depósito de información privilegiada
	Flujos de aprobación
	Notificaciones y alertas
	Informes y Dashboards
	Análisis de comportamiento
	Logs y Auditoría
	Autenticación
	Gestión de usuarios y perfiles
	Gestión y grabación de sesiones
	Gestión de certificados digitales
	Automatización de tareas privilegiadas
	Elevación de privilegios
	Descubrimiento de credenciales
	Análisis de comportamiento
	Secret Management
	Entorno de instalación

No	DETALLE DE FUNCIONES REQUERIDAS
	Condiciones generales
1	La solución deberá soportar, como mínimo 200 sesiones simultáneas
2	La solución deberá soportar, como mínimo, 4,500 horas de almacenamiento de grabación de sesiones
3	Los usuarios gestionados por la solución pueden estar conectados simultáneamente
	La Solución debe permitir el almacenamiento seguro y control de credenciales no personales y privilegiadas en servidores Linux/Unix, Windows (incluyendo cuentas de servicio como COM+ e IIS), sistemas, aplicaciones web, bases de datos, estaciones de trabajo y dispositivos de red, con un total de 25 usuarios o 1000 dispositivos
5	Proporcionar una autenticación transparente en el sistema o dispositivo de red de destino. La solución debe iniciar una sesión introduciendo directamente las credenciales en la pantalla de inicio de sesión y sirviendo de proxy para la sesión entre el usuario y el sistema de destino, de modo que la contraseña no quede expuesta al solicitante de acceso.

6	Eliminar las credenciales insertadas en el código fuente, los scripts y los archivos de configuración, haciendo que las contraseñas sean gestionadas por la solución e invisibles para los desarrolladores y el personal de soporte de TI
7	Generar videos o registros de texto de las sesiones realizadas a través de la solución, almacenados en un depósito seguro, cifrado y protegido contra cualquier alteración que comprometa la integridad de estas pruebas.
	Arquitectura de la solución y sistema de respaldo
8	La solución debe gestionar todo el entorno sin necesidad de instalar agentes o cualquier software en los sistemas de destino o dispositivos de red
9	El modelo de licencia de la aplicación no debe restringir su uso en caso de que se alcance el límite de licencia contratado
10	La solución deberá generar videos o registros de texto de las sesiones realizadas a través de la solución, almacenados en un depósito seguro, encriptado y protegido contra cualquier alteración que comprometa la integridad de estas pruebas
11	La solución deberá permitir la generación automática de contraseñas de alta complejidad de acuerdo con las reglas de cada tecnología y la Política de Seguridad de la institución.
12	Tanto los dispositivos como los sistemas operativos que componen la solución deben seguir los estándares de «hardening» actualizados constantemente por el fabricante de la solución del depósito de contraseñas y protegidos con firewall interno y detección de intrusos
13	La base de datos se debe suministrar como parte integral de la solución
14	La solución debe utilizar una base de datos con las mejores prácticas de seguridad, debe estar en un entorno "hardenizado", con mecanismo de blindaje y criptografía del sistema operativo y documentación que acredite la contemplación de estos requisitos
15	No permitirse en ningún caso la apertura del depósito con claves criptográficas generadas por sus respectivos proveedores y/o fabricantes
16	La solución debe permitir el uso de la encriptación de la base de datos utilizada por la solución para almacenar las contraseñas de las credenciales gestionadas por ella, y también debe ser compatible con al menos uno de los siguientes métodos y estándares de encriptación: a) AES con claves de 256 bits; b) FIPS 140-2; c) Encriptación PKCS# 11 o superior por hardware utilizando dispositivos HSM debidamente homologados por el fabricante para la solución ofrecida
17	Para las operaciones de autenticación y acuerdo de clave de sesión, debe permitir el uso de algoritmos del sistema de criptografía de clave pública RSA de al menos 2048 bits
18	Para la generación de hash, debe permitir el uso del algoritmo SHA-256 o variaciones superiores de la familia SHA-2
19	La solución debe ofrecer mecanismos para cifrar el usuario y la contraseña de conexión a la base de datos
20	La solución no debe traficar con datos sensibles en texto claro
21	La solución debe proporcionar mecanismos de encriptación de la información sensible almacenada en la base de datos compatibles con el estándar AES con claves de 256 bits
22	La interfaz de la solución, cuando se accede a través del navegador web, debe utilizar el protocolo HTTPS
23	La copia de seguridad/recuperación de todos los datos y configuraciones de la solución debe estar incluida y debe permitir al administrador programar copias de seguridad para una fecha y hora determinadas y exportarlas a un servidor SFTP remoto
24	La solución debe mantener la persistencia de todos los informes y archivos históricos, incluyendo las grabaciones de las sesiones, sin necesidad de restaurar las copias de seguridad, durante al menos 90 (noventa) días
25	La solución debe permitir la conservación en copia de seguridad de los informes y registros de la aplicación durante al menos 2 (dos) años

26	La solución debe permitir la conservación en copia de seguridad de las grabaciones de las sesiones durante al menos 6 meses
27	El archivo de copia de seguridad no debe contener ninguna información de la cuenta y la contraseña en texto claro
28	A la hora de realizar la copia de seguridad de la clave maestra, el sistema debe poder dividirla en un número parametrizado de partes, de forma que no permita que una sola persona pueda ver la totalidad, sino sólo la parte que le corresponde a cada una de ellas
29	La solución debe permitir la replicación en otros Centros de Datos
30	En caso de falla de uno de los servidores del clúster del depósito de contraseñas de alta disponibilidad local, cada uno de los servidores deberá gestionar todas las solicitudes de acceso sin ninguna pérdida de rendimiento o funcionalidad
31	La solución debe permitir al administrador utilizar la opción de replicación asíncrona entre los nodos de la solución de depósito de contraseñas, si así lo desea
32	Los cambios realizados en el clúster local de alta disponibilidad de la cámara acorazada de contraseñas deben replicarse automáticamente a los otros servidores de redundancia, de forma sincrónica y con un retraso (delay) máximo de 50ms.
33	La solución deberá utilizar tecnología de restricción y autenticación que incluya la firma digital (Hash), y la dirección IP del host o conjunto de hosts a los que se va a acceder con la solución
	Administración de la solución
34	La solución debe tener todas las funciones proporcionadas por el mismo fabricante, sin depender de herramientas o adaptaciones de terceros
35	Posibilidad de comunicarse con los servicios de directorio a través del protocolo LDAP y LDAPS
36	Posibilidad de implementar MIB II, según RFC 1213
37	La solución debe tener una única interfaz, en la misma solución, para gestionar las contraseñas y las sesiones
38	La solución debe ofrecer el aprovisionamiento y la gestión de todas las cuentas privilegiadas, incluidas las cuentas para la administración de aplicaciones empresariales, bases de datos y dispositivos de red, sin limitarse únicamente a las cuentas del sistema operativo de los servidores
39	La solución debe sincronizar la fecha y el reloj a través de NTP (Network Time Protocol) o del servicio de fecha y hora del sistema operativo
40	La solución debe proporcionar mecanismos de actualización de seguridad: a) De forma automática; b) A demanda
41	Disponer de una consola de configuración unificada para gestionar las cuentas y los activos añadidos al depósito de contraseñas
42	Permitir la copia de seguridad y recuperación de su base de datos, así como las configuraciones de software establecidas, con las siguientes capacidades: a) Permitir la ejecución de las tareas de copia de seguridad y encriptación sin necesidad de agentes de terceros, proporcionando así el mayor nivel posible de seguridad e integridad de los datos a respaldar; b) Permitir la ejecución de copias de seguridad automatizadas a través de la programación/agenda de horarios.
43	Permitir, a través de una interfaz gráfica, que los administradores configuren integraciones con dispositivos y/o plataformas que no se proporcionan de forma nativa, sin necesidad de servicios profesionales de terceros
44	Extraer copias de seguridad del sistema, registros y videos, así como las credenciales a un servidor ubicado en los Centros de Datos remotos en caso de que sea necesario restaurar todas las configuraciones y datos de a solución de bóveda de contraseñas.
	Gestión de contraseñas

45	La solución debe permitir la parametrización de las políticas de seguridad y fortaleza de las contraseñas por parte del administrador del sistema, entre ellas: conjunto de caracteres alfanuméricos, numéricos y especiales, pudiendo además elegir qué caracteres especiales se permitirán, con la posibilidad de no permitir caracteres repetidos, generando contraseñas aleatorias.
46	La solución debe contar con la funcionalidad para gestionar claves SSH y escanear servidores Linux e identificar y publicar claves SSH.
47	La solución debe permitir realizar el cambio automático de contraseñas, en horarios programados, después de que hayan sido liberadas para su uso o por expiración del plazo
48	La solución debe permitir la consolidación periódica de las contraseñas para identificar las contraseñas que han sido cambiadas en los sistemas gestionados
49	La solución debe permitir la posibilidad de gestionar contraseñas privilegiadas en las aplicaciones e integración con los sistemas heredados
50	La solución debe ofrecer una interfaz con vista personalizada exclusiva para Auditorías y Organismos Reguladores, que contenga los dispositivos y credenciales gestionados por la solución
51	La solución debe proporcionar un área de transferencia segura, para que el solicitante pueda ver la contraseña o copiarla en la pantalla de inicio de sesión del sistema de destino
52	La solución debe permitir liberar o revocar automática e inmediatamente todos los accesos de una determinada credencial
53	La solución debe permitir enviar notificaciones por correo electrónico o SMS sobre las nuevas solicitudes de aprobación de acceso a los respectivos responsables de las credenciales;
54	La solución debe permitir el control en línea del uso de las cuentas y la desconexión de la sesión;
55	La solución debe presentar la función "break glass" para el acceso de emergencia a las cuentas, es decir, permitirá el acceso a los activos protegidos de manera urgente, sin necesidad de aprobación previa en las cuentas a las que el usuario no tendría acceso, sin pérdida de rastreo;
56	La solución debe frecer la función "Discovery" para buscar nuevos servidores, elementos de red y bases de datos, siendo capaz de levantar automáticamente las cuentas creadas en estos nuevos dispositivos, incluyendo la posibilidad de descubrir los certificados SSL utilizados en los dispositivos gestionados.
57	La solución debe ofrecer la posibilidad de bloquear comandos específicos, con la opción de detener la sesión si el usuario ejecuta un comando inapropiado
58	La solución debe permitir realizar búsquedas por comandos específicos ejecutados por el usuario a través de la línea de comandos en los registros o sesiones grabadas
59	La solución debe permitir realizar la configuración de alertas inmediatas cuando ciertos comandos son ejecutados por usuarios con privilegios
60	La solución debe ofrecer la posibilidad de generar informes basados en los registros y exportarlos a archivos en formato ".csv"
61	La solución debe permitir al administrador configurar la comunicación con aplicaciones de terceros utilizando scripts, macros, llamadas ejecutables, varios lenguajes de programación y aceptar varios protocolos incluyendo, al menos, RPC, WinRM, SSH, API REST HTTP/HTTPS
62	Las contraseñas generadas automáticamente por la solución de depósito de contraseñas deben cumplir los siguientes requisitos: a)Poder determinar la cantidad de caracteres; b) Estar compuesta por números, letras mayúsculas, minúsculas y caracteres especiales; c) Poder predefinir los caracteres especiales que se pueden utilizar; d) Aleatorias, de modo que dentro del historial de una cuenta sea poco probable encontrar dos contraseñas iguales; e) Que no se basen en palabras del diccionario

63	La solución debe permitir la creación de políticas de contraseñas de forma jerárquica o en niveles de seguridad, permitiendo la creación de contraseñas diferentes para grupos de activos de diferentes plataformas o criticidades
64	La solución debe disponer de un mecanismo para exportar el archivo con las últimas contraseñas al repositorio remoto, encriptado y protegido por contraseña de doble custodia para la recuperación de la contraseña en caso de fallo total de la solución
65	La solución debe habilitar políticas de contraseñas que impidan la visualización simultánea de credenciales, sesiones, así como configurar el tiempo de caducidad de las contraseñas en función de la visualización y la fecha de caducidad. Se debe poder elegir los días de la semana y las horas en que las credenciales pueden caducar.
66	La solución debe gestionar las contraseñas de las aplicaciones privilegiadas para evitar la situación de las contraseñas integradas en el código fuente.
67	La solución debe tener la capacidad de gestionar credenciales que se encuentran en sistemas ubicados en múltiples ubicaciones geográficas o dominios distintos;
68	La solución debe poder gestionar las contraseñas de las aplicaciones privilegiadas, para evitar las contraseñas integradas en los códigos fuente.
69	La solución no debe depender de la instalación de agentes para cambiar las contraseñas.
70	La solución debe restablecer la credencial (contraseña) en el entorno para los casos de visualización de la contraseña por parte del solicitante en los procesos de verificación de credenciales.
	Rotación de contraseñas
71	La solución debe permtir realizar el cambio automático de contraseñas para servidores (Unix, Linux, Windows), bases de datos (MS SQL, ORACLE, MYSQL, PostgreSQL), Aplicaciones Web, Dispositivos de Red;
72	La solución debe permitir la generación automática de contraseñas de fuerza/complejidad según las reglas de cada tecnología y la Política de Seguridad de la institución
73	La solución debe permitir la flexibilidad para la configuración de la fuerza de la contraseña generada
74	La solución debe permitir realizar el cambio automático de contraseñas, en horarios programados, después de que hayan sido liberadas para su uso o por expiración del plazo
75	La solución debe permitir la Posibilidad de gestionar contraseñas privilegiadas en las aplicaciones e integración con los sistemas heredados
76	La solución debe permitir el almacenamiento de historial de contraseñas por equipo
77	La solución debe permitir el registro de los cambios realizados
78	La solución debe permitir generar informes de seguimiento de los cambios realizados
79	La solución debe permitir generar informes de errores en los cambios
80	La solución debe emitir alertas de fallas o de éxito de los cambios;
81	La solución debe contar con la posibilidad de reconfigurar/personalizar scripts o plug-in de intercambio de contraseñas para la configuración de casos que requieran parámetros específicos para la rotación de contraseñas;
82	La solución debe permitir realizar la configuración de políticas de cambio de contraseñas con agenda programada o por ocurrencia de eventos con especificación de parámetros de tiempo para el cambio;
83	La solución debe proporcionar plantillas de intercambio de contraseñas que se puedan abrir, editar y auditar;
84	La solución de contar con plantillas con lenguaje accesible y de fácil interpretación;
85	La solución debe permitir realizar la trazabilidad de los cambios de plantilla;
86	La solución debe permitir realizar el cambio de contraseñas en aplicaciones HTTP/HTTPS con plantillas

	Control de acceso
87	La solución debe poder limitar la ejecución de comandos críticos por parte de los usuarios registrados.
88	La solución debe poder proporcionar acceso externo sin necesidad de instalar un agente o utilizar una VPN
89	La solución debe permitir el control de la ejecución de comandos críticos mediante, al menos, "whitelist" y "blacklist".
90	La solución debe tener un tiempo de expiración de la sesión configurable por el administrador del sistema.
91	La solución debe permitir la parametrización del número máximo de sesiones activas por usuario.
92	La solución debe soportar la desconexión de la sesión debido a la actividad/mal uso de los comandos pre-registrados en el sistema.
93	La solución debe permitir la creación de grupos de usuarios.
94	La solución debe permitir implementar bloqueo o alerta de comandos con alertas, interrupción de la sesión o sólo el registro de la ejecución - Basado en blacklist;
95	La solución debe permitir realizar el bloqueo o alerta de comandos con alertas, interrupción de la sesión o sólo registro de ejecución - Basado en whitelist;
96	La solución debe permitir la posibilidad de bloquear y auditar comandos específicos;
97	La solución debe permitir realizar búsquedas por comandos específicos ejecutados por el usuario a través de la línea de comandos en los registros o sesiones grabadas;
98	La solución debe permitir implementar la configuración de alertas inmediatas cuando ciertos comandos son ejecutados por usuarios con privilegios;
99	La solución debe permitir la clasificación de las puntuaciones de los comandos según el nivel de riesgo de cada uno de ellos.
100	La solución debe permitir la asignación de privilegios a grupos de usuarios asociados a uno o varios objetivos gestionados.
101	La solución debe permitir la integración con las herramientas de gestión de incidentes (ITSM) para validar los tickets abiertos durante el proceso de aprobación del acceso
102	La solución debe permitir el acceso simultáneo de dos o más usuarios al depósito de contraseñas y a las cuentas privilegiadas.
103	La solución debe permitir la segregación de funciones entre usuarios de una misma aplicación gestionada.
104	La solución debe proporcionar la función de revocar todos los accesos de un usuario registrado de forma inmediata.
105	La solución debe permitir el acceso simultáneo de dos o más usuarios a las credenciales privilegiadas.
106	El acceso simultáneo a credenciales, contraseñas y dispositivos no debe comprometer la trazabilidad.
	Integraciones y compatibilidad
107	Habilitar, vía script, la creación de nuevos conectores basados en accesos SSH y RDP, de manera que sea posible soportar nuevas interfaces para la autenticación de activos.
108	La solución debe permitir el acceso a través de dispositivos móviles como tablets y smartphones.
109	La solución debe ser compatible con los sistemas operativos: Windows Server 2008 o superior, Red Hat Enterprise, Debian, CentOS, Solaris.
110	La solución debe ser compatible con las aplicaciones de Windows: cuentas de servicio y grupos de aplicaciones de IIS

111	La solución de ser compatible con los sistemas de gestión de bases de datos: Oracle, Oracle RAC, MSSQL, MySQL, MongoDB, PostgreSQL;
112	La solución debe ser compatible con dispositivos de seguridad a través de protocolo HTTP/HTTPS
113	La solución debe ser compatible con dispositivos de red: Cisco, D-Link, HP, 3com, Alcatel, Brocade, ARUBA, Huawei.
114	La solución debe ser compatible con aplicaciones: WebLogic, JBOSS, Tomcat, Peoplesoft, Oracle Application Server, Apache e IIS.
115	La solución debe ser compatible con servicios de Directorios: AD, LDAP, LDAPS
116	La solución debe ser compatible con entornos virtuales: Hyper-V, Vmware.
117	La solución debe ser compatible con storages
118	La solución debe contener un SDK (kit de desarrollo de software) o una API (interfaz de programación de aplicaciones) que se pueda configurar para que las aplicaciones de los clientes puedan:
119	a) Solicitar credenciales y dispositivos;
120	b) Registro y modificación de credenciales y dispositivos;
121	c) Solicitar claves SSH;
122	d) Registro y modificación de claves SSH.
123	La solución debe ser compatible con aplicaciones en la nube como ser Rackspace, IBM SmartCloud, Microsoft Azure, Hyper-V, Google Cloud Platform, GoGrid, Vmware vCenter Server, Amazon AWS.
Registro de activos	
124	La solución debe permitir el registro manual parametrizado de los equipos;
125	Atributos como Marca, Modelo, Fabricante, Localidad, Grupo abiertos a la configuración por parte del administrador de la herramienta independientemente del fabricante.
Depósito de información privilegiada	
126	La solución debe permitir el almacenamiento de certificados digitales;
127	La solución debe permitir el almacenamiento de contraseñas personales;
128	La solución debe emitir alertas de vencimiento de información almacenada;
129	La solución debe generar registros de cambios de información privilegiada;
Flujos de aprobación	
130	La solución debe ser flexible en el proceso de aprobación del acceso a las cuentas privilegiadas (accesos previamente aprobados, accesos con aprobación única y accesos con aprobaciones multinivel).
131	La solución debe permitir la configuración de flujos de aprobación diferenciados según el grado de criticidad y las características de la cuenta, como las cuentas privilegiadas y las cuentas utilizadas por terceros.
132	La solución debe permitir al aprobador cambiar el periodo de acceso solicitado por un usuario.
133	En caso de aprobarse una solicitud de acceso, la sesión y el privilegio concedidos deben expirar automáticamente al final del período autorizado.
134	La solución debe permitir acceder al flujo de solicitudes y aprobaciones de forma remota y segura.
135	La solución debe tener una función para revocar todos los accesos de una persona de forma inmediata.
136	La solución debe poder comparar los accesos concedidos y registrados en su base con los accesos realmente realizados en un activo. Después de la comparación, el sistema debe mostrar las incoherencias encontradas en un informe, como por ejemplo un ingreso realizado en el activo pero no autorizado en la solución.

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

137	La solución debe proporcionar un campo para introducir un número de identificador de solicitud o cambio al que se asociará el acceso.
138	La solución debe ofrecer una interfaz para usuarios y auditores, proporcionando mecanismos flexibles de control de acceso para crear vistas/grupos personalizados de dispositivos gestionados y cuentas privilegiadas.
139	La solución debe proporcionar un mecanismo de acceso de emergencia para retirar las contraseñas registradas en la solución.
140	La activación del acceso de emergencia debe notificarse a los aprobadores por correo electrónico o por la interfaz de la herramienta.
	Notificaciones y alertas
141	Las notificaciones o alertas emitidas por la solución deben ser personalizables.
142	La solución debe permitir el envío de alertas por parte del SIEM para contraseñas que no coinciden con las del depósito.
143	La solución debe ser configurable para enviar alertas activadas por el sistema, al menos por correo electrónico y SNMP, para eventos personalizados por el administrador del sistema que incluyan al menos uno de los siguientes servicios:
144	a) Si se detienen los servicios esenciales
145	b) Cuando se alcanza el límite de procesamiento de la CPU
146	c) Cuando se alcanza el límite de procesamiento de la memoria
147	d) Cuando se alcanza el límite de capacidad de almacenamiento de datos
148	La solución debe poder notificar, por correo electrónico, las nuevas solicitudes de acceso a los responsables de su aprobación.
149	La solución debe poder notificar al solicitante de acceso, por correo electrónico, los accesos que fueron o no aprobados.
150	Las notificaciones deben ser configurables para que el administrador de la solución pueda activarlas o desactivarlas individualmente.
	Informes y Dashboards
151	La solución debe permitir que los módulos de visualización de la sesión y de generación de informes muestren el número de registros localizados y la compaginación de resultados para cada búsqueda realizada.
152	La solución debe permitir la generación de informes de todos los usuarios registrados en la aplicación, y sus respectivos roles.
153	La solución debe permitir la generación de informes de las cuentas de usuarios privilegiados monitoreadas por la herramienta.
154	La solución debe contar con mecanismos para generar informes sobre las cuentas privilegiadas, como listas de activos y sus cuentas gestionadas, solicitudes de acceso a cuentas privilegiadas presentadas para su aprobación, aprobadas o rechazadas, y el historial de uso de las cuentas privilegiadas.
155	Los informes deberán exportarse, como mínimo, a los siguientes formatos: PDF, XLSX y CSV.
156	La solución debe registrar las actividades administrativas, como las modificaciones de políticas y cuentas.
157	La solución debe informar la última fecha de cierre de sesión para cada cuenta privilegiada, para identificar las cuentas que ya no pueden ser utilizadas.
158	La solución debe proporcionar una lista de las cuentas de usuario habilitadas cuya contraseña no se ha cambiado durante más de 30 días.
159	La solución debe proveer un historial detallado de todos los cambios de seguridad de contraseñas realizados en los dispositivos por cualquier usuario.
160	La solución debe permitir hacer un listado de todas las cuentas gestionadas por la solución junto con los detalles de la edad de la contraseña

161	La solución deberá permitir generar un listado de las cuentas de usuario de activos, filtrados por ubicación, estado, asociación de grupo, etc.
162	La solución debe proporcionar una vista transaccional detallada de las actividades de las sesiones de los dispositivos.
163	La solución debe proporcionar una lista con los detalles de la actividad de desbloqueo de la contraseña de la solución.
164	La solución debe proporcionar los detalles de la actividad de actualización de las contraseñas de la solución.
165	La solución debe proporcionar los detalles de las próximas actualizaciones programadas de las contraseñas.
166	La solución debe proporcionar una lista detallada de los sistemas que utilizan una cuenta de servicio de solución para iniciar uno o más servicios.
167	La solución deberá almacenar el historial de uso de las credenciales, así como cualquier otro tipo de acción asociada a su uso, como la gestión remota, el cierre de sesión del administrador, etc. El historial se puede ver dentro de la propia solución o mediante la generación de informes de auditoría.
168	La solución debe permitir generar informes de funcionamiento con una lista de usuarios, equipos y credenciales registradas;
169	La solución debe permitir generar informes PCI;
170	La solución debe permitir generar informes de Gestión de Eventos;
171	La solución debe permitir generar informes de Auditoría;
172	La solución debe permitir generar informes de Alertas;
173	La solución debe presentar dashboard de utilización;
174	La solución debe presentar dashboard de conexiones;
175	La solución debe presentar Dashboard de utilización de sesiones;
176	La solución debe presentar Dashboard de sesión;
177	La solución debe presentar Dashboard de usuario;
178	La solución debe presentar Dashboard de servidor;
179	La solución debe presentar Dashboard de estación de acceso.
180	La solución debe presentar Dashboard de amenazas en tiempo real
181	La solución debe controlar el acceso a los informes en función de los permisos configurados en la solución.
182	La solución debe permitir registrar cada acceso, incluidos los accesos a la aplicación web para solicitudes de contraseña, aprobaciones, salidas, cambios de delegación, informes y otras actividades. El acceso a la consola de gestión, tanto para la configuración como para los informes, debe quedar registrado, así como todas las actividades de cambios de contraseña.
183	La solución debe proporcionar datos programados ad hoc, informes en tiempo real sobre los usuarios, cuentas, configuración del dispositivo e información sobre los procesos del mismo.
184	La solución debe proporcionar informes con visibilidad jerárquica, que contengan listas y filtros de clasificación para que los usuarios puedan profundizar en la información y los recursos a los que desean acceder.
	Análisis de Comportamiento
185	La solución deberá realizar análisis de la sesión del usuario basado en el historial de comportamiento. Análisis mínimo de las variables de la estación de origen, las estaciones de destino, las credenciales, los tiempos, la duración de la sesión;
186	La solución deberá realizar la identificación de comportamientos diferenciados con alertas de anormalidad en informes en pantalla o alertas para SIEM/SYSLOG;

187	La solución deberá realizar el análisis de sesión de usuario con puntuaciones de comandos críticos con alertas de anormalidad en informes en pantalla o alertas a SIEM/SYSLOG;
188	La solución deberá presentar dashboards gráficos con información sobre riesgos y amenazas
	Logs y Auditoría
189	La solución debe permitir la integración con herramientas SIEM de acuerdo con los estándares del mercado, mediante el servicio de información o el envío automático de logs a servidores SYSLOG, adhiriéndose a los principios del RFC 5424.
190	La solución debe tener una pista de auditoría de la aplicación de las reglas para cada cuenta de acceso privilegiado.
191	La solución debe permitir el seguimiento de todas las acciones realizadas en los sistemas gestionados por cuentas privilegiadas.
192	El sistema debe registrar todas las actividades realizadas y poner los datos de auditoría a disposición de los usuarios con el perfil adecuado, como el de Auditor.
193	La solución debe alertar al usuario de que la sesión está siendo grabada, y el banner de alerta puede ser personalizado por el administrador de la solución.
194	La solución debe proporcionar un mecanismo de búsqueda de registros de acceso a los activos.
195	La solución debe permitir la búsqueda de comandos específicos ejecutados por el usuario, como en las sesiones SSH y Windows.
196	El mecanismo de registro debe ser suministrado y desarrollado como parte integral de la solución, y no se aceptarán programas de fabricantes distintos al desarrollador de la solución propuesta.
197	La solución debe ser capaz de almacenar los videos de las sesiones en un repositorio seguro, cifrado y protegido contra cualquier alteración que comprometa la integridad de estas pruebas.
198	La solución debe comprimir los vídeos grabados. Además, se utilizan técnicas de compresión para los periodos de inactividad de la sesión.
199	La solución debe poder grabar la sesión del usuario en vídeo, independientemente de la forma de acceso.
200	La solución debe controlar el acceso a las sesiones grabadas, tanto en forma de permiso como registrando quién ha tenido acceso.
201	La solución debe soportar la búsqueda de comandos ejecutados y vincular estos comandos a los marcos de las sesiones grabadas y almacenadas.
202	La solución debe permitir la expiración y depuración de las grabaciones de forma automática o manual.
203	La solución debe permitir almacenar y exportar las grabaciones a ubicaciones externas a PAM (red local o nube).
	Autenticación
204	La solución debe permitir una autenticación transparente en el sistema objetivo, con un inicio de sesión mediante la inyección directa de credenciales.
205	La solución debe permitir la autenticación de usuario multifactorial (MFA).
206	Debido a las vulnerabilidades de seguridad y a la necesidad de integración con los servicios de telefonía, la autenticación multifactorial no debe utilizar SMS.
207	La solución debe integrarse con soluciones de autenticación de dos factores, incluidos los tokens de tiempo y certificados digitales de los tipos A1 y A3.
208	La solución debe integrarse con la base de usuarios con privilegios administrativos de Microsoft Active Directory, TACACS y RADIUS para conceder acceso a la plataforma y también para asignar perfiles de acceso a las funciones del sistema.
209	La solución deberá permitir la autenticación centralizada integrada con el protocolo SAML;
210	La solución deberá permitir la autenticación centralizada integrada con protocolo OpenID;

211	La solución deberá permitir la autenticación centralizada integrada con autenticación por certificado digital personal para usuarios y administradores;
212	La solución deberá permitir la autenticación nativa de dos factores para el acceso a la web o al cliente;
213	La solución debe poder bloquear a los usuarios y sesiones que se encuentren dentro de las siguientes características de acceso:
	a) Acceso inusual a un dispositivo;
	b) Acceso de origen inusual;
	c) Acceso inusual a una credencial;
	d) Acceso de duración inusual;
	e) Acceso a horarios inusuales.
214	La solución debe permitir la autenticación local mediante usuarios y contraseña;
215	La solución debe permitir la autenticación centralizada integrada con LDAP, LDAPS para MS AD con múltiples DCS.
	Gestión de usuarios y perfiles
216	La solución deberá permitir el registro de usuarios con información tal como nombre, correo electrónico y departamento como mínimo
217	La solución deberá permitir el registro de perfiles de usuario
218	La solución debe permitir la segregación de funciones por perfiles de acceso
219	La solución deberá permitir la flexibilidad para crear cualquier perfil nuevo, con varias combinaciones de pantallas y funciones según la necesidad del negocio sin la intervención del proveedor
220	La solución deberá permitir la creación de TAGs personalizados para definir dispositivos y credenciales
221	La solución deberá permitir la importación automática de cuentas de usuario desde AD
222	La solución deberá permitir la importación automática de cuentas de usuario desde LDAP;
223	La solución deberá permitir la gestión de grupos y perfiles de acceso integrados con grupos AD/LDAP.
	Gestión y grabación de sesiones
224	La solución debe permitir la gestión y el seguimiento de las sesiones establecidas mediante protocolos: HTTP, HTTPS, SSH y RDP, ya sea a través de un proxy o Jump Server.
225	La solución debe permitir el seguimiento en tiempo real de las sesiones o actividades de los usuarios privilegiados, disponible en una interfaz centralizada (Dashboard).
226	La solución debe garantizar el seguimiento de las actividades realizadas con cuentas de acceso privilegiado obtenidas en caso de emergencia ("break-glass").
227	La solución debe poder registrar las sesiones de los usuarios privilegiados.
228	La grabación de sesión de usuario debe admitir la grabación de video continua de toda la sesión.
229	La grabación de la sesión debe permitir la grabación de la interacción del mouse y del teclado durante la sesión.
230	La solución debe soportar la grabación de sesiones de usuarios simultáneos. La cantidad máxima de sesiones debe basarse en el hardware utilizado para la solución, no debe tener una limitación de software.
231	Las grabaciones de las sesiones se deben almacenar en formato encriptado. Las grabaciones deberán almacenarse en formato comprimido.
232	La solución debe permitir la gestión y monitorización de las sesiones de redes sociales, a las que se accede a través del navegador, como Facebook, Twitter, Instagram y Linkedin.
233	La solución no debe depender de la instalación de agentes para grabar la sesión.
234	La solución debe realizar la grabación de video de las sesiones realizadas a través de webproxy o proxy transparente en formato optimizado;
235	La solución debe realizar la grabación de comandos tecleados en entornos RDP y SSH;

236	La solución debe permitir ver el video de una sesión celebrada directamente en la solución, sin necesidad de convertirlo a formato de video o descargarlo;
237	La solución debe permitir exportar la sesión en formato de video;
238	La solución debe permitir la búsqueda del registro de sesión por usuario, sistema de destino, ip de destino, fecha y hora;
239	La solución debe permitir la búsqueda de comandos y entradas de teclado introducidos en la plataforma Linux;
240	La solución debe permitir la búsqueda de comandos y entradas de teclado en la plataforma Windows;
241	La solución debe permitir la grabación de registros de entrada y salida de comandos;
242	La solución no requiere agentes locales para la grabación de sesiones
243	Almacenamiento y consulta de registros que proporcionen al menos, la siguiente información:
244	a) Identificación del usuario que realizó determinado acceso a un dispositivo;
245	b) Identificación de quien aprobó el acceso del usuario;
246	c) Fecha y hora del acceso realizado y de las acciones que el usuario realizó en el dispositivo remoto.
247	La solución debe proporcionar al menos los siguientes filtros para la recuperación de registros: Usuario; Sistema objetivo accedido, Tipo de actividad, Intervalo de tiempo (fecha/hora/minuto de inicio y fin);
248	La solución debe permitir el seguimiento en línea de las sesiones remotas por parte del administrador y la desconexión de la sesión remota;
	Gestión de certificados digitales
249	La solución deberá gestionar el ciclo de vida completo de un certificado, con las siguientes funciones: Creación de una solicitud, firma, renovación y revocación de certificados.
250	La solución deberá gestionar certificados en las siguientes plataformas: Windows, Linux, CA Microsoft, Cisco y certificados web.
251	La solución debe contar con flujos de aprobación, incluida la aprobación multinivel para las siguientes funciones: Firma de un .csr, renovación e instalación.
252	La solución deberá realizar la implementación de certificados en los siguientes entornos como mínimo: Apache, IIS, Nginx, Tomcat
253	La solución debe permitir la revocación de un certificado, no permitiendo ninguna interacción con el certificado cuando es revocado, sólo su renovación.
254	La solución debe contar con informes de gestión y cuadros de mando que muestren toda la base de certificados, centralizando la información más crítica sobre un certificado, como los que están a punto de caducar.
255	La solución debe permitir la configuración de notificaciones multinivel como, por ejemplo, un certificado a 90 días de caducidad lo notificará al analista, a 60 días de caducidad lo notificará al gestor, y a 30 lo notificará al gestor.
256	La solución debe permitir la creación e importación de solicitudes de certificados (.csr).
257	La solución debe integrarse con al menos las siguientes autoridades de certificación: DigiCert, Godaddy, Microsoft CA, Comodo, GlobalSign y Let's Encrypt
258	La solución validará la información del certificado basándose en normas personalizadas. Los certificados que no se ajusten a estas normas serán considerados inválidos por el sistema.
259	La solución debe permitir retirar la contraseña de un certificado en función de los permisos asignados a cada usuario. Todos los retiros deben ser auditados, y también debe ser posible pasar por un proceso de flujo de aprobación con break the glass y aprobación multinivel.
260	La solución deberá permitir el registro de información genérica en el certificado como TAGS para que esta información sea considerada al momento de otorgar el acceso a los certificados.

261	La solución deberá permitir la ejecución de acciones por etapas, como revocación, renovación, inactivación y verificación de certificados revocados.
262	La solución deberá permitir la creación de organizaciones de gestión de certificados dentro del sistema.
263	La solución debe contar con informes de gestión y cuadros de mando que muestren toda la base de certificados, centralizando la información más crítica sobre un certificado, como los que están a punto de caducar.
264	La solución debe permitir la importación manual de un certificado, independientemente de su formato.
265	La solución debe poder enviar certificados por correo electrónico en los principales formatos, siendo como mínimo: der, pem, pfx, p7b.
266	La solución debe poder descargar certificados en los principales formatos, siendo como mínimo: der, pem, pfx, p7b.
267	La solución debe permitir la gestión de los certificados independientemente del formato que tengan. Esta información debe ser transparente para el administrador.
268	La solución debe tener una función para delegar a un responsable, que será notificado ante cualquier evento relacionado con ese certificado.
269	La solución debe contar con dashboards gestionables que muestren todos los certificados activos gestionados, separando por varios tipos de reglas de negocio, como vencimiento, nivel de seguridad y ubicación de los certificados.
270	La solución debe permitir la renovación de certificados, y también debe poder cambiar la información sobre un certificado y generar un historial para un posible registro de información.
271	La solución debe integrarse con al menos una entidad validadora de certificados revocados, como por ejemplo OCSP.
272	La solución debe permitir la instalación programada de un certificado, pudiendo seleccionar el día, la hora y la fecha en que se instalará, y también en qué dispositivos se instalará dicho certificado.
273	La solución debe tener una función para renovar automáticamente los certificados cuando el certificado estuviera: X días antes de la fecha de vencimiento, en la fecha de vencimiento y X días después de la fecha de vencimiento.
274	La solución deberá disponer de un sistema para evaluar la seguridad de un certificado, teniendo en cuenta al menos 5 criterios de seguridad.
275	La solución debe gestionar los certificados de forma que no se tenga en cuenta el formato de los mismos, es decir, en la solicitud, firma, renovación e instalación de los certificados, el administrador no debe saber qué formatos se requieren, esto debe estar incorporado en la inteligencia de la aplicación.
	Automatización de tareas privilegiadas
276	La solución debe realizar la ejecución de tareas con scripts pre-registrados, haciendo posible la elección de múltiples dispositivos para el mismo script.
277	La solución debe permitir registrar una variable para sustituir las credenciales en el script de ejecución, para no exponer las credenciales que se utilizarán en las ejecuciones.
278	La solución debe contar con un flujo de trabajo de aprobación para la ejecución de tareas, incluyendo la aprobación multinivel con al menos tres niveles.
279	La solución debe permitir la creación de variables para la ejecución, definiendo los nombres de las variables y sus valores, como por ejemplo, al registrar el script: echo'VARIABLE', la ejecución será echo'valor de la variable'.
280	La solución debe tener informes con el historial de ejecuciones, indicando qué script se ejecutó, en qué dispositivos, si hubo algún error y quién fue el solicitante.
	Elevación de privilegios
281	La solución debe permitir el retiro de la contraseña de las credenciales del cliente, basándose en los permisos registrados en el servidor.

282	La solución debe permitir la elevación de una solicitud.
283	La solución debe tener whitelist para aplicaciones.
284	La solución debe realizar el descubrimiento de las aplicaciones instaladas en la máquina y también permitir al usuario registrar nuevas aplicaciones para realizar una actualización.
285	La solución debe permitir la elevación de las funciones del panel de control, como la realización de cambios en la fecha y la hora y la región.
286	La solución debe permitir la segregación de las funciones del panel de control, permitiendo que diferentes usuarios ejecuten diferentes funciones del panel de control.
287	La solución debe hacer un listado de todos los adaptadores de red en el ordenador, pero también permitir la elevación de un adaptador, permitiendo cambios en la configuración.
288	La solución debe hacer un listado de todos los programas instalados en la computadora, y también permitir la desinstalación de una aplicación.
289	La solución debe tener modo offline, pudiendo almacenar una caché de credenciales para su ejecución en caso de indisponibilidad del servidor.
290	La solución debe permitir el registro de nuevas versiones, para que se actualicen automáticamente en las estaciones de trabajo de los usuarios.
291	La solución debe restringir el movimiento lateral y cualquier salida de conexión, ya sea RDP o SSH.
292	La solución debe bloquear la elevación de procesos hijos si el proceso hijo está en la lista blanca, como abrir CMD y desde CMD abrir PowerShell.
293	La solución debe permitir la automatización de inicios de sesión y tareas, como por ejemplo identificar una página web de Facebook, e insertar las credenciales sin que el usuario conozca la contraseña utilizada.
294	La solución debe contar con un dashboard administrativo, que muestre al menos el número de dispositivos y usuarios que utilizan la herramienta en el recinto, y también un gráfico que contenga el uso cuantitativo de las elevaciones.
295	Cuando se aprueba un usuario, debe ser posible añadir una fecha de vencimiento o un plazo para utilizar la solución, para facilitar la gestión del acceso de terceros.
296	Un usuario puede utilizar la aplicación en más de un dispositivo, y un dispositivo puede tener más de un usuario registrado. Los permisos deben basarse en el dispositivo y el usuario, es decir, un usuario puede ejecutar el Panel de Control en la máquina A pero no puede ejecutarlo en la máquina B.
297	Este tipo de acceso no revela ninguna contraseña al usuario;
298	La solución debe permitir, de forma detallada, decidir qué aplicaciones se guardarán en el proceso de elevación de privilegios.
299	Realiza la grabación del registro en el depósito.
300	Verificar el riesgo de ejecución de un archivo basado en la integración con plataformas de validación;
301	Permite simular las acciones de los usuarios, creando acciones macro, para automatizar el inicio de sesión en las aplicaciones instaladas;
302	Todas las ejecuciones de la aplicación se deben registrar y presentar en un informe centralizado, siendo posible filtrar por tipo de ejecución o evento.
303	La solución debe controlar los permisos de cada función, permitiendo la segregación de las funciones de la herramienta para varios grupos de usuarios diferentes, sin necesidad de una instalación adicional.
304	La solución debe controlar la elevación de privilegios en las estaciones de trabajo (endpoints), para ejecutar las aplicaciones autorizadas que requieren este privilegio ("Run As");
305	Posibilidad de mapear los recursos compartidos de red con un usuario administrador, diferente del usuario conectado a la máquina ("Mapear como").

306	Si se separa en componentes, ninguno de ellos debe contener contraseñas en texto claro para la autenticación;
	Descubrimiento de credenciales
307	La solución debe poder encontrar dispositivos de red y credenciales, de al menos los siguientes entornos:
	a) Servidores Linux/Unix, Windows y VMWare;
	b) Base de datos Oracle, SQL y MySQL;
	c) Dispositivos de red como firewalls, enrutadores, conmutadores y balanceadores;
	d) Puestos de trabajo.
308	La solución debe poder realizar la detección en todos los dominios, encontrando dispositivos y credenciales en Active Directory.
309	La solución debe realizar el descubrimiento de certificados en los siguientes entornos, como mínimo: Apache, Nginx, Tomcat, IIS, Directorios (Linux y Windows), Workstations windows (certstore), Certificados HTTPS y Certificados emitidos por CA Microsoft
310	La solución deberá realizar el descubrimiento de plataformas DevOps de como mínimo:
	a) Dockers - Contenedores;
	b) Ansible - Playbooks y roles;
	c) Jenkins - Trabajos, nodos y usuarios;
	d) Kubernetes - Secrets.
311	La solución debe realizar el descubrimiento de las cuentas de servicio de Windows, así como identificar qué dispositivos están utilizando la cuenta.
312	La solución debe contar con un dashboard o informe que haga un listado del progreso de la ejecución de los descubrimientos, incluyendo su barra de progreso.
313	1.18.7. La solución debe poder escanear continuamente los dispositivos, proporcionando información sobre accesos sospechosos o indebidos, como el acceso al dispositivo con credenciales que no están registradas en el depósito, o el acceso desde fuera de la solución PAM.
314	1.18.8. La solución debe permitir el descubrimiento de las cuentas privilegiadas utilizadas en los servicios web de forma automática o mediante adaptaciones a través de un script integrado en el SDK o API de la solución. Por ejemplo: aplicaciones basadas en Microsoft IIS.
315	1.18.9. La solución debe poder descubrir, almacenar y gestionar automáticamente las claves SSH en los sistemas Linux.
316	1.18.10. La solución debe permitir el descubrimiento continuo, es decir, debe poder registrar días y horas para la reejecución de un descubrimiento, incluyendo la selección de períodos y días que se ejecutarán.
	Análisis de Comportamiento
317	La solución debe tener un sistema de evaluación basado en la puntuación para evaluar los accesos sospechosos, críticos y no habituales al sistema.
318	La solución debe tener criterios de evaluación como mínimo de las siguientes características de acceso:
	a) Acceso no habitual a un dispositivo;
	b) Acceso de origen no habitual;
	c) Acceso no habitual a una credencial;
	d) Acceso de duración no habitual;
	e) Acceso de horario no habitual."
319	La solución debe poder bloquear a los usuarios y las sesiones que se encuentren dentro de las siguientes características de acceso:
	a) Acceso no habitual a un dispositivo;
	b) Acceso de origen no habitual;
	c) Acceso no habitual a una credencial;
	d) Acceso de duración no habitual;

	e) Acceso de horario no habitual."
320	La solución debe contar con un informe que centralice toda la información sobre los comandos bloqueados que se han intentado ejecutar.
	Secret Management
321	La Solución debe ser totalmente compatible con los sistemas, servicios y aplicaciones que se ejecutan en Docker Containers, y debe realizar la gestión de secretos en entornos DevOps y contenedores, almacenando de forma segura secretos, contraseñas, claves criptográficas, tokens o cualquier otro valor necesario, considerando los siguientes aspectos:
322	Soporte para al menos 60 aplicaciones que se ejecutan dentro de cada contenedor distribuido, entre los clusters mencionados en el punto anterior.
323	La solución debe permitir que los pods/contenedores se autentiquen y luego obtengan la autorización a través del espacio de nombres/proyecto y la cuenta de servicio de los orquestadores de contenedores o de Oauth y obtengan acceso seguro sólo a los secretos que les pertenecen.
324	La solución debe encriptar las claves privadas SSL que son utilizadas por cualquiera de los servicios de la solución, o que se utilizan en la encriptación de la base de datos para evitar que se almacenen en texto claro en el sistema de archivos.
325	La solución debe permitir que las aplicaciones que se ejecutan dentro de los contenedores tengan un acceso seguro a los secretos para su uso efectivo.
326	La solución debe rotar los secretos, cuando sea aplicable, tanto en términos de complejidad como de tiempo de caducidad, según las políticas que se definan en la propia herramienta.
327	La solución debe proporcionar medios para revocar completamente el acceso a un secreto a petición o mediante la definición de políticas.
328	La solución debe garantizar una alta disponibilidad a través de la replicación de secretos en al menos 2 nodos diferentes de la solución para asegurar que, en caso de que uno de ellos se detenga, el otro asumirá automáticamente sus funciones;
329	La solución debe ofrecer una interfaz de administración web para la gestión y la elaboración de informes sobre el clúster y los distintos componentes de la solución;
330	La solución debe permitir al menos los siguientes métodos de autenticación: Usuario y contraseña, LDAP y Radius;
	Entorno de instalación
331	La solución debe basarse en un dispositivo virtual que cumpla las siguientes especificaciones:
	a) Si la base de datos y/o el sistema operativo utilizados son de terceros (ejemplo: ORACLE/SQL o Windows), la solución debe entregarse con las licencias de software y la garantía que la hace compatible con la solución;
	b) En el caso anterior, la empresa contratada deberá también dar soporte a los componentes adicionales que se entreguen, directamente o mediante subcontratación, sin ningún coste adicional para el CONTRATISTA;
	c) No es necesario utilizar herramientas de terceros para completar la solución, es decir, un único fabricante que satisface todas las necesidades de un depósito de contraseñas.
332	Arquitectura de implementación de la solución
	a) La solución debe tener licencia y ser implementada para cumplir, como mínimo, con los siguientes requisitos de arquitectura: Se instalará en 02 (dos) lugares;
	b) Para que la solución siga funcionando a nivel local incluso con la falla de un nodo de cada elemento, en cada una de las 02 (dos) ubicaciones, se deben instalar al menos los siguientes elementos en régimen de alta disponibilidad:
	i) Depósito de Contraseñas (entendido como el elemento de la solución que controla las credenciales de acceso, incluida la interfaz de acceso de los usuarios a la solución); - Gateway/Proxy de Sesión (elemento que proporciona y controla el acceso privilegiado supervisado a los activos de TI);
	ii) La solución debe replicar las configuraciones en ambas ubicaciones para que, en caso de falla total de sus elementos instalados en una ubicación, la solución siga estando disponible mediante el uso de elementos en la otra ubicación;

ESPECIFICACIONES TECNICAS PARA LA ADQUISICIÓN DE SUSCRIPCION DE SOFTWARE DE SEGURIDAD PARA EL PARCHEO VIRTUAL PARA SERVIDORES INSTITUCIONALES Los ofertantes deberá detallar en su oferta si cumplen con lo siguiente:
Cantidad de Licencias: Adquisición de suscripción de software de seguridad para el parcheo virtual para 22 servidores institucionales.
Nombre del producto: Software de seguridad para el parcheo virtual para servidores institucionales.
Tipo de Licenciamiento: Suscripción Anual
Idioma: Español
Producto entregable: Documento de adquisición de la suscripción que especifique la cantidad de Licencias que se están habilitando al 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.
Período de suscripción y activación de las licencias: 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

	d) El modelo mínimo de funcionamiento y de tolerancia a fallas a ser implementado es:
	i) Sitio Web principal: Activo;
	ii) Sitio Web secundario: Activo;
	e) El acceso primario (en situaciones normales) de los usuarios a la solución debe ser siempre a través de los elementos instalados en su red local.

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

Anexo de Contrato No. 30021, Oferta de Compra No. 350, 23/12/2022

ÍTEMS N° 5

FIREWALL PARA APLICACIONES WEB (WAF)

ESPECIFICACIONES TECNICAS PARA LA ADQUISICIÓN DE SUSCRIPCION DE LA SOLUCIÓN DE FIREWALL PARA APLICACIONES WEB EXTERNAS Los ofertantes deberá detallar en su oferta si cumplen con lo siguiente:
Cantidad de Licencias: Adquisición de una suscripción de la solución de firewall para aplicaciones web externas.
Nombre del producto: Firewall para aplicaciones web externas
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.
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

No	FUNCIONES REQUERIDAS EN LA SOLUCIÓN DE FIREWALL PARA APLICACIONES WEB (WAF) EXTERNAS
I.	Dimensionamiento
I.	Condiciones Generales
II.	Despliegue
IV.	DDOS
V.	**Dashboard y gestión**
VI.	Seguridad
VII.	BOTs
VIII	**Reputación de la IP**
IX	Analítica avanzada
X	**Integración**
IX	CDN
XII	Monitoreo
XIII	**Protección de APIs**
XIV	**Protección DNS**
XV	**Balance de carga**

FUNCIONES A REALIZAR POR LA SOLUCIÓN DE FIREWALL PARA APLICACIONES WEB EXTERNAS

Los ofertantes deberán detallar en su oferta si la solución cumple con las funciones siguientes:

NO.	DETALLE DE FUNCIONES REQUERIDAS
1	**DIMENSIONAMIENTO**
1.1	La solución requerida tiene como propósito proteger 1 sitio
1.2	Se estima que el tráfico total de las aplicaciones a proteger es de 16 Mbps
2	**CONDICIONES GENERALES**
2.1	Se requiere un servicio brindado desde la nube para la protección de los sitios web de la organización ante ataques a la capa aplicativa (Web Application Firewall) capaz de contener ataques como SQLi, XSS, CSRF, RFI, etc. listados en el informe de OWASP.
2.2	La solución debe ser operada mediante una interfaz gráfica WEB proporcionado por el proveedor de la solución
2.3	La solución debe ser líder en el mercado por más de 5 años, para lo cual se considerarán los informes de Gartner (Magic Quadrant de WAF/WAAP) y Forrester (DDoS Mitigation Solution Wave)
2.4	La solución debe permitir incluir los certificados y llaves originales de los sitios o proporcionar sin costo adicional los certificados digitales para los sitios a proteger
2.5	La solución debe almacenar por lo menos 30 días de eventos registrados
2.6	La solución debe contar con la función que obligue el uso de HTTPS (en caso de requerirse) para los sitios protegidos
2.7	La solución ofertada no debe cotizar por separado ni cobrar cargos extra por la inclusión de reglas personalizadas o "custom", tanto de seguridad como de caché y gestión del contenido.
2.8	La gestión de actualizaciones de la solución y de firmas será realizada por el fabricante.
3	**DESPLIEGUE**
3.1	La solución debe ser provista en un esquema 100% de nube, sin la necesidad de implementación de elementos (tanto de hardware como de software) en el Centro de Datos de la Institución
3.2	La solución debe soportar esquemas de implementación híbridos, mediante la integración de WAF on-premise de la misma marca. Esta característica no debe ser obligatoria para el correcto funcionamiento de la solución en nube
3.3	La infraestructura de la organización debe contar con más de 50 puntos de presencia desde las cuales se brindan los servicios de la solución a contratar. Los puntos de presencia deben contar con todas las funcionalidades solicitadas. No se tendrán en cuenta puntos de presencia que (por ejemplo) solo cuenten con la funcionalidad de CDN
3.4	La solución ofertada deberá operar sin mayores cambios en la infraestructura, pudiendo redireccionarse el tráfico de los aplicativos WEB mediante el cambio en los servidores DNS
4	**DDOS**
4.1	La solución ofertada debe ser capaz de mitigar ataques de denegación de servicio hacia las aplicaciones de manera automatizada para las capas 3,4 y 7 del modelo OCI
4.2	La solución debe ser capaz de detectar DDoS capa 7, específico para cada aplicación web protegida
4.3	La solución debe estar en la capacidad de bloquear ataques de DDoS de cualquier tamaño, frecuencia y duración. Ningún ataque de DDoS debe generar costos adicionales para la Institución.
4.4	Se deben poder definir parámetros (umbrales) de detección de condiciones de DDoS para cada uno de los sitios protegidos
4.5	Se deben poder excluir bots "benignos" como motores de búsqueda, Site Helpers, B2B API clients, etc.

4.6	La solución debe proteger de ataques de DDoS de manera distribuida y transparente, sin necesidad de redireccionar el tráfico a POPs o Puntos de Presencia específicos ante ataque, generando latencias y problemas de propagación y ruteo. Todos los POPs deben contar con todas las funciones (Aceleración, WAF, Protección DDoS, etc).
4.7	La solución debe estar en la capacidad de mitigar los ataques de DDoS en no más de tres segundos
4.8	La mitigación de los ataques de DDoS debe ser automatizada y "multi-vector"
5	**DASHBOARD Y GESTIÓN**
5.1	La solución debe poder registrar alertas tanto de seguridad, cambios de configuración y estado de la plataforma.
5.2	La solución debe proveer dashboards en tiempo real del estado de cada uno de los aplicativos protegidos, incluyendo:
	- Tráfico en tiempo real
	- Cantidad de clientes accediendo a la aplicación
	- Cantidad de requests
	- Cantidad de bloqueos
	- Alertas de seguridad
	- Tráfico "ahorrado" por métodos de cache y compresión
	- RTT a datacenters de origen
	- Alertas de estado y ataques
	- Auditoría de cambios de configuración
5.3	La solución debe permitir indagar en tiempo real los distintos eventos de seguridad, incluyendo los datos de los request individuales que han sido bloqueados o permitidos, los criterios evaluados y el detalle del request particular, con la posibilidad de buscar y filtrar por diferentes criterios.
5.4	La solución debe poder comunicar eventos mediante envío de correos de alertas a los destinatarios definidos mediante configuración
5.5	La solución debe permitir agregar usuarios de gestión y visualización, para que tengan acceso a la consola
5.6	Los usuarios deben poder integrar múltiples factores de autenticación para loguearse/firmarse a la solución ofertada
5.7	La solución debe generar reportes periódicos de seguridad
5.8	La solución debe permitir la gestión mediante interface WEB como así también integración mediante API tanto para cambios de configuración como para monitoreo de estado, permitiendo alcanzar la mayoría de las funcionalidades mediante ambos métodos de acceso
5.9	La solución debe registrar e informar los cambios realizados por cada uno de los usuarios, con la finalidad de permitir la trazabilidad de actividades de gestión
6	**SEGURIDAD**
6.1	La solución debe detectar ataques aplicativos de seguridad, incluyendo los mencionados en los informes de OWASP (SQL Injection, Command Injection, Remote File Inclusion, Cross Site Scripting, Cross Site Request Forgery, etc).
6.2	La solución debe informar y alertar los ataques aplicativos, pudiendo definir por política para cada aplicación, qué acciones tomar ante dichos eventos (ejemplo: bloquear el request individual, sólo alertar, bloquear la IP, etc.)
6.3	La solución debe proteger ante ataques de dia cero, sin impacto de falsos positivos
6.4	La solución debe incluir la posibilidad de definir reglas personalizadas de seguridad, utilizando los criterios necesarios y sintaxis lógica para definición de los casos particulares. Estos criterios deben incluir sin limitarse, al menos los siguientes:
	- Dirección IP de origen
	- País de origen (geolocalización)

	- Existencia de header particular, evaluación de valores
	- Existencia y valor de cookies
	- Tipo de cliente (tipo de bot, humano, api client, etc)
	- Métodc HTTP utilizado
	- Númerc de request dentro de la sesión
	- Parámetros y valores
	- Parámetros y valores
	- URL y URIs
	- Cantidad de hits
	- User Agent
	- Referer
	- Post Data
	- Tamaño del Request
	- Session request rate
	- ASN de origen
6.5	La solución debe permitir tomar acciones personalizadas para las reglas de seguridad, incluyendo bloqueos de sesión, request, envio de Captchas
6.6	La solución debe llevar métricas y contadores, así como contabilizar en las alertas en tiempo real, los eventos identificados mediante las reglas personalizadas de seguridad
6.7	Las reglas y cambios de configuración de seguridad deben propagarse en tiempo real o "near-real time" con un tiempo máximo para tomar efecto a nivel global de 1 minuto
6.8	La solución debe permitir especificar whitelists o exclusiones para los controles, incluyendo parámetros como URLs, direcciones IP de origen, países, etc.
6.9	La solución debe contar con los mecanismos necesarios para procurar la reducción de falsos positivos al máximo. Los mecanismos deben ser automatizados, es decir, sin la necesidad de intervención humana, tanto por parte del personal interno como del proveedor de la solución
6.10	La solución deberá contar con funcionalidades que permitan:
	- Rastrear e identificar las fuentes de los ataques originadas desde proxies anónimos, direcciones ip maliciosas, botnets y sitios de phishing.
	- Actualizar las fuentes de ataque para identificar y bloquear el tráfico malicioso.
	- Ajustar dinámicamente las políticas de seguridad con base en la identificación de las fuentes de ataque o de las fuentes que denoten actividad sospechosa.
	- Bloquear solicitudes de acceso basado en la reputación de la fuente del tráfico, como direcciones IP conocidas por su comportamiento malicioso por Botnet, DDoS, Phishing o redes de Anonimización (TOR y Proxies Anónimos).
	- Bloquear solicitudes de acceso basado en el país de origen de la conexión.
	- Realice un análisis automático de distribución de alertas en relación al país de origen, con opción a representar la información a través de un mapa mundial
	- Detallar y analizar los eventos de seguridad ocurridos, orígenes y método del ataque, dirección IP y localización geográfica del ataque.
6.11	La solución debe soportar las últimas versiones de TLS y permitir la definición de protocolos soportados de manera estricta
6.12	La solución deberá cubrir todas las vulnerabilidades expresadas en el OWASP Top Ten más reciente sin requerir de algún tipo de configuración específica para tener la protección
6.13	La solución deberá proteger tanto las aplicaciones Web HTTP, como las aplicaciones web SSL y HTTPS.
	- La solución deberá tener la capacidad de recibir y utilizar los certificados y pares de llaves público/privadas para los servidores web protegidos.

	- La solución deberá desencriptar el tráfico SSL, de las aplicaciones web, entre el cliente y el servidor y re-encriptarlo antes de su reenvío.
7	**BOTs**
7.1	La solución debe ser capaz de identificar bots (scripts automatizados sin interacción humana) accediendo a los sitios de manera transparente (sin afectar la experiencia de usuario original).
7.2	La solución debe clasificar los bots por tipo y permitir tomar acciones diferentes en base a este criterio, así como llevar estadísticas por sitio o aplicativo protegido
7.3	La solución debe permitir la detección de bots sin la necesidad de integrar código en las aplicaciones de cliente.
7.4	La solución debe contar con algoritmos complejos y actulizados de detección y c asificación de bots y herramientas automatizadas
7.5	La solución debe informar el porcentaje de bloqueos en tiempo real y acciones tomadas ante la presencia de Bots y herramientas automatizadas
7.6	La solución debe prevenir el uso de bots del estilo "comment spammers"
7.7	La solución debe proteger ante el uso de herramientas de escaneo automatizadas
7.8	La solución debe proteger ante ataques automatizados mediante herramientas de scripting y librerías de hacking.
8	**REPUTACIÓN DE LA IP**
8.1	La solución debe incluir sus propias métricas de reputación de IP, incluyendo detalles como tipos de ataques perpetrados por dichos orígenes en el pasado
8.2	La solución debe mantener información de geo-localización de los orígenes.
9	**ANALÍTICA AVANZADA**
9.1	La solución debe hacer análisis de los ataques, agregando eventos y alertas individuales en incidentes o "narrativas" de ataques y amenazas, incluyendo detalles útiles para el análisis de los ataques dirigidos, por ejemplo:
	- Herramientas utilizadas
	- Direcciones IP de origen y porcentaje de ataque por cada una
	- Vectores de ataque
	- Aplicaciones y recursos atacados
	- Historial en el tiempo, incluyendo eventos bloqueados y/o alertados
	- Muestra de eventos
	- Análisis estadístico
	- Integración con información de inteligencia (geolocalización, ataques conocidos, etc)
9.2	La solución debe contar con un módulo que a través de algoritmos de Machine Learning correlacione los eventos dándoles un contexto, asignación de severidad y categorización de los mismos
10	**IINTEGRACIÓN**
10.1	La solución debe permitir el envío de dichas alertas a correlacionadores on-premise/cloud que utilicen el protocolo syslog (como herramientas SIEM). Debe proveer formatos reccnocidos y que se puedan integrar en informes o "apps" sin necesidad de desarrollo por parte del cliente
10.2	Debe integrarse de manera "nativa" con tecnologías de correlación de eventos reconocidas de mercado, como Splunk, IBM QRadar, ArcSight
10.3	La solución propuesta debe contar con APIs (Web Services tipo REST) que permitan automatizar tareas administrativas y/o la integración con otros elementos dentro de la organización
11	**CDN**
11.1	La solución debe brindar la posibilidad de acelerar el contenido mediante caché de elementos estáticos y dinámicos
11.2	La solución debe perfilar y aprender automáticamente las políticas de caching para cada elemento, en manera especial para contenido dinámico generado

11.3	La solución debe permitir la definición del/los puntos de presencia más cercanos a los datacenters de origen para cada aplicación, con el fin de utilizar algoritmos de caché de capas múltiples, ruteo dinámico inteligente del contenido y reutilización del backbone de la CDN para acelerar el contenido a clientes remotos, reduciendo el RTT desde puntos de presencia (POPs) lejanos. La Infraestructura debe tener más de 50 Puntos de Presencia
11.4	La solución debe permitir medición de la performance de la aceleración del contenido, pudiendo revisar los tiempos, decisiones de caching o forward-to-origin para cada elemento particular de cada página
11.5	Se deben poder generar reglas customizadas de cache, incluyendo objetos a cachear o no cachear, por cuanto tiempo, basados en criterios de URL
11.6	La propagación global de actualizaciones y reglas de cache debe ser en tiempo real o "near real time", nunca excediendo el minuto, al igual que las directivas de purga de caché
11.7	Las técnicas combinadas de caché y aceleración deben incluir al menos:
	- Validacion asíncrona
	- Minificación de contenido CSS, JS y HTML
	- Compresión de imágenes
	- Compresión de contenido "on the fly"
	- Pre-Pooling de conexiones TCP
11.8	Debe incluir opciones de configuración avanzadas como:
	- Cumplir optativamente con directrices de "no-cache" o "max-age" de parte de los clientes
	- Cumplir con headers "Vary"
	- Utilizar la duración mínima de cache ante conflictos
	- Preferir "last modified" por sobre "eTag"
	- Deshabilitar la posibilidad de caching en el cliente
	- Cachear las respuestas de headers 3XX (ej. redirecciones perpetuas)
	- Caching basado en headers de respuesta
11.9	La solución debe soportar HTTP/2 y permitir transformar automáticamente a éste protocolo aplicaciones legacy HTTP/1.1
11.10	La solución ofertada debe poder acelerar el delivery del contenido de las aplicaciones WEB
12	**MONITOREO**
12.1	La solución debe monitorear los servidores de origen del contenido con el fin de determinar su disponibilidad y la capacidad de re-dirigir el tráfico a servidores disponibles
12.2	La solución debe permitir configurar los parámetros de monitoreo por aplicación, incluyendo qué URLs monitorear, qué respuesta esperar, cuánto tiempo de timeout, intervalos de verificación.
12.3	La solución debe alertar ante eventos de caída de servicio o falta de llegada a os servidores protegidos
13	**PROTECCIÓN DE APIs**
31.1	La solución debe contar con un módulo específico que permita detectar y mitigar ataques dirigidos contra las APIs de la organización (Web Services tipo REST). El módulo debe contar con un tablero de control propio
14	**PROTECCION DNS**
14.1	La solución debe proporcionar un mecanismo de protección para los servidores DNS con los que cuenta la organización y también contar con la posibilidad de que la organización pueda administrar directamente los DNS en la solución del proveedor. Los dos mecanismos se deben proporcionar para que la organización decida en cualquier momento cual es la mejor opción. Por cada sitio contratado se debe permitir la gestión o protección de por lo menos 10 zonas de DNS
15	**BALANCE DE CARGA**
15.1	La solución ofertada debe permitir balancear por cada sitio a por lo menos dos IPs públicas

2. JUSTIFICACIÓN DE LA UNIDAD SOLICITANTE

2.1 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.

2.2 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.

BOLPROS PRODUCTOS DE EL SALVADOR, 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

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

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:

Anexo de Contrato No. 30021, 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 nstitución, indicando teléfono, correo electrónico y nombre de la persona de contacto, dicha información podrá ser verificado por el CNR, con las nstituciones 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**
	a) 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, S.A. de C.V. BOLPROS

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.**

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. 30021, Oferta de Compra No. 350, 23/12/2022

FORMULARIO DE PRECIOS SIN IVA Y CON IVA

ANEXO 7

Contrato	30021		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
2	SUSCRIPCIÓN DE SOFTWARE DE SEGURIDAD PARA LA PROTECCIÓN DE LA BASE DE DATOS INSTITUCIONAL.	1	$ 158,200.00	$ 158,200.00	$ 178,766.00	$ 178,766.00
3	SOLUCIÓN DE SEGURIDAD PARA LA GESTIÓN DE ACCESOS CON PRIVILEGIOS.	1	$ 31,150.00	$ 31,150.00	$ 35,199.50	$ 35,199.50
5	FIREWALL PARA APLICACIONES WEB (WAF).	1	$ 17,450.00	$ 17,450.00	$ 19,718.50	$ 19,718.50
TOTAL CONTRATO				$ 206,800.00		$ 233,684.00

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

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

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

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