**ACUERDO No. 148-CNR/2021.** El Consejo Directivo del Centro Nacional de Registros, sobre lo tratado en el **punto número siete: Unidad de Adquisiciones y Contrataciones Institucional. Subdivisión siete punto dos:** Bolpros 02-/2021-CNR Ítem #1 Servicios de renovación de suscripción de la solución para la orquestación, automatización y respuesta a incidentes de seguridad (SOAR) y de la solución antispam y filtrado de mensajes de correo electrónico, entrante y saliente, institucional, año 2021. Oferta de compra No. 329; de la sesión ordinaria número dieciocho celebrada en forma virtual y presencial, a las catorce horas del diecinueve de agosto de dos mil veintiuno; punto expuesto por el jefe de la Unidad de Adquisiciones y Contrataciones Institucional –UACI-Licenciado Andrés Rodas Gómez, y

**CONSIDERANDOS:**

**I)** Que mediante Acuerdo N° 86-CNR/2020, de fecha 12 de noviembre de 2020, el Consejo Directivo, autorizó el inicio del proceso N° BOLPROS-02/2021-CNR denominado "Servicios de renovación de suscripción de la solución para la orquestación, automatización y respuesta a incidentes de seguridad (SOAR) y de la solución antispam y filtrado de mensajes de correo electrónico, entrante y saliente institucional, año 2021", para el período del 1 de enero al 31 de diciembre de 2021, por medio de la aplicación de los procedimientos de la Bolsa de Productos y Servicios, y una comisión del 1% más IVA, a cancelarse en un solo pago sobre el monto total contratado en BOLPROS, S.A. DE C.V., para lo cual se instruyó a la Administración, efectuar las acciones que fueren necesarias para cumplir el debido procedimiento legal; así mismo, en dicho acuerdo se nombró como Administrador del Contrato al Ingeniero Juan José Rivas Ángel, Oficial de Seguridad Informática, de la Dirección de Tecnología de la Información, designando a la Directora Ejecutiva nombrar a otro Administrador del Contrato, cuando por alguna situación especial fuera necesario.

**II)** Que mediante Acuerdo N° 37-CNR/2021, de fecha 11 de febrero de 2021, el Consejo Directivo, acordó: I) Darse por recibido del informe sobre los resultados del proceso BOLPROS-02/2021-CNR denominado "Servicios de renovación de suscripción de la solución para la orquestación, automatización y respuesta a incidentes de seguridad (SOAR) y de la solución antispam y filtrado de mensajes de correo electrónico, entrante y saliente institucional, año 2021", desarrollado por medio de la bolsa, con la Oferta de Compra N° 329, contratado con el proveedor TRUST NETWORK, S.A. DE C.V., por un valor total de USD$51,697.50 con IVA incluido, para el plazo según negociación y contratación en Bolpros, a partir del 1 de enero hasta el 31 de diciembre de 2021 y una Comisión Bursátil del 1% más IVA equivalente USD$516.98 dólares, sumando un total de USD$52,214.48 dólares con IVA incluido (contratación, ítem 2 Servicios de Renovación de Suscripción de Solución Antispam y Filtrado de Mensajes de Correo Electrónico); II) Autorizar a la Dirección Ejecutiva, a la Unidad de Adquisiciones y Contrataciones Institucional y a la Dirección de Tecnología de la Información, continuar con el proceso de la adquisición por medio de Bolpros del ítem # 1 "Solución para la Orquestación Automatización y Respuesta a Incidentes de Seguridad (SOAR)", *por las razones indicadas*. **III)** Aprobar la modificación a los Términos de Referencia para continuar con el proceso por medio de Bolpros, (en la parte de las cartas o constancias de referencia, para que no se solicite incluir el monto de las contrataciones y en la parte de distribuidor autorizado que se incorpore la condición de proveedores redistribuidores o canales de distribución por ser uno de los términos que el propietario de dicha aplicación está utilizando para los distribuidores de su producto en El Salvador). IV) Modificar el plazo de la contratación para el período de 12 meses a partir del cierre de la negociación y contratación.

**III)** Que en fecha 23 de noviembre de 2020, se emitió Orden de Negociación N° 383/2020 y se realizó la publicación de la Oferta de Compra N° 329, ITEM # 1 en fecha 1 de marzo de 2021 por medio del sitio web de Bolpros;

**IV)** Que mediante Requerimiento N° 13612 de fecha 29 de octubre de 2020, se solicitó a la UACI realizar las gestiones correspondientes para contratar los "Servicios de renovación de suscripción de la solución para la orquestación, automatización y respuesta a incidentes de seguridad (SOAR) y de la solución antispam y filtrado de mensajes de correo electrónico, entrante y saliente Institucional, año 2021", de acuerdo al siguiente detalle:

| N° de ítem | Servicio |
|---|---|
| 1 | SERVICIOS DE RENOVACIÓN DE SUSCRIPCIÓN DE LA SOLUCIÓN PARA LA ORQUESTACIÓN, AUTOMATIZACIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD (SOAR) |

**V)** Que la oferta se evaluó, de acuerdo al criterio establecido en el siguiente cuadro:

| PARÁMETRO | CONDICIÓN | EVALUADOR |
|---|---|---|
| Evaluación de las especificaciones técnicas por ítem. | CUMPLE/NO CUMPLE | Unidad Solicitante |

El CNR se reservó el derecho de implementar los mecanismos necesarios para verificar la información presentada por el participante.

**VI)** Que en fecha 4 de marzo de 2021, se recibió de parte de BOLPROS la oferta de 1 participante, la cual fue sometida a evaluación técnica, obteniéndose el siguiente resultado:

| N° | NOMBRE DEL PUESTO DE BOLSA VENDEDOR | CÓDIGO DEL CLIENTE / EMPRESAS OFERTANTES | ÍTEMS A PARTICIPAR |
|---|---|---|---|
| 1 | Multiservicios Bursátiles, S.A. | 01329 / TRUST NETWORK, S.A. DE C.V. | ITEM # 1 |

**VII)** Que se procedió a revisar la oferta técnica presentada, tomando los parámetros establecidos en la Oferta de Compra N° 329 modificada, por lo que la unidad solicitante, verificó el cumplimiento de las condiciones establecidas en los criterios de evaluación técnica en la oferta, obteniéndose el siguiente resultado:

| ITEM N° 1 SERVICIOS DE RENOVACIÓN DE SUSCRIPCIÓN DE LA SOLUCIÓN PARA LA ORQUESTACIÓN, AUTOMATIZACIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD (SOAR). | TRUST NETWORK S.A. DE C.V. | | |
|---|---|---|---|
| | **CUMPLE** | **NO CUMPLE** | **OBSERVACIONES** |
| Presentar carta vigente del fabricante, firmada por el(los) fabricante(s) o de su representante o del representante regional para Latinoamérica, o presentar cuenta de correo electrónico para corroborar la veracidad y validez en la cual establezca que el Oferente es distribuidor o redistribuidor autorizado en El Salvador, de conformidad a las regulaciones del proveedor, para comercializar Starlight Bundle: Data Processorm Sensors and Agents, en la cual haga constar que se compromete a brindar soporte técnico durante la vigencia del contrato. | X | | Se validó carta con fabricante |
| **EXPERIENCIA DEL PROVEEDOR** | | | **OBSERVACIONES** |
| El proveedor deberá presentar al menos UNA (1) cartas o constancias de referencia originales o fotocopias simples, emitidas en un período no mayor a TRES (3) meses antes de la fecha de la invitación para presentar ofertas y 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 al servicio igual al solicitado 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, monto contratado o facturado si fuere permitido o indicar que no se puede proporcionar por la confidencialidad de la información, 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 (en el caso del sello si aplica), por el respectivo Titular o Autoridad o Director o Gerente o Encargado de la Administración del Contrato u órdenes de compra de la Institución o empresa, indicando teléfono, correo electrónico y nombre de la persona de contacto, según ANEXO N° 4.<br>Se aceptaran cartas o constancias de referencia emitidas por una misma Institución o empresa siempre y cuando se haga constar la experiencia de 1 a 3 contratos u órdenes de compra dentro de los últimos 3 años.<br>Dicha información podrá ser corroborada por la Unidad solicitante con las entidades emisoras, en caso de presentar fotocopias simples. | X | | Presentó carta de referencia del Centro Nacional de Registros |
| **ESPECIFICACIONES TECNICAS** | **CUMPLE** | **NO CUMPLE** | **OBSERVACIONES** |
| Cantidad de Licencias: Renovación de Suscripción de una solución para la Orquestación Automatización y Respuesta a Incidentes de Seguridad (SOAR) | X | | |
| Nombre del producto: Starlight Bundle: Data Processor Sensors and Agents, solución para la Orquestación Automatización y Respuesta a Incidentes de Seguridad (SOAR) | X | | |

| | | | |
|---|---|---|---|
| Tipo de Licenciamiento: Suscripción Anual | X | | Se previno el período de vigencia del contrato, la vigencia de la suscripción de la solución ofertada y el servicio de soporte técnico y mantenimiento y fue subsanado a través de nota de fecha 22/3/2021 |
| Producto entregable: Documento de renovación de la suscripción que especifique la solución adquirida | X | | |
| Soporte Técnico y Mantenimiento: Carta compromiso que manifieste que el tiempo de atención del soporte y mantenimiento es bajo la modalidad 7x24 (7 días a la semana, 24 horas al día) de lunes a domingo.<br>- Soporte técnico mediante acceso remoto ilimitado<br>- Soporte técnico mediante llamadas telefónicas o correo electrónico ilimitado | X | | Se previno y fue subsanado |
| **ASPECTOS GENERALES** | | | **OBSERVACIONES** |
| 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 les acredite. | X | | Se previno y fue subsanado presentando atestados del personal certificado en la solución |
| 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. | X | | |
| **FUNCIONES QUE REALIZAR POR LA SOLUCIÓN PARA PARA LA ORQUESTACIÓN AUTOMATIZACIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD (SOAR) Los ofertantes deberán detallar en su oferta si la solución cumple con las funciones siguientes:** | **CUMPLE** | **NO CUMPLE** | **OBSERVACIONES** |
| 1. La solución debe estar basada en una solución de virtual appliance con sistema operativo propietario, securizado y optimizado de fábrica. Se debe implementar tanto en ambiente virtual y la nube. | X | | Se previno y fue subsanado |
| 2. La solución debe permitir tener múltiples sensores incluyendo sensores de seguridad, de red y de servidores | X | | |
| 3. La solución debe permitir una capacidad de procesamiento de datos por día 100 GB. Durante la vigencia del contrato podría variar el servicio debido a la necesidad de incrementar capacidad de procesamiento de datos por día. | X | | |
| 4. La solución debe poseer la funcionalidad de administrar varias tenants (ambientes) desde una misma consola de gestión, sin necesidad de licenciamiento adicional. | X | | |
| 5. Debe ejecutar aprendizaje vía ML (Machine Learning) y AI (Artificial Intelligence) | X | | |
| 6. La solución debe proveer la capacidad de ejecutarse por servicios administrados con dashboards y casos de uso ilimitados, ejecutar actualización de búsquedas sin licenciamiento adicional. | X | | |
| 7. La solución debe ajustar alertas basadas en cada etapa de Cybersecurity basada en KillChain | X | | |
| 8. Proveer descripción por cada malware detectado | X | | |

| **FUNCIONES QUE REALIZAR POR LA SOLUCIÓN PARA PARA LA ORQUESTACIÓN AUTOMATIZACIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD (SOAR) Los ofertantes deberán detallar en su oferta si la solución cumple con las funciones siguientes:** | **CUMPLE** | **NO CUMPLE** | **OBSERVACIONES** |
|---|---|---|---|
| 9. La solución debe ser capaz de extraer información granular entendible para el usuario a nivel de metadata en las capas 2 a 7 de la capa TCP/IP | X | | |
| 10. Los sensores debe ser capaces de capturar información de toda la red y solo enviar información relevante al dashboard para análisis. | X | | |
| 11. La solución debe proveer funcionalidad de Machine Learning Supervisado y no Supervisado | X | | |
| 12. La solución debe proveer la funcionalidad de procesar los datos por medio de AI y ML | X | | |
| 13. La solución debe incluir sensores IDS integrados sin licenciamiento adicional | X | | |
| 14. Para garantizar un análisis granular de las muestras, identificando ataques desconocidos / de 0 días, el motor de análisis debe poder reproducir la ejecución de malware en un emulador de máquina que reproduce un hardware virtual, incluida una CPU emulada. La CPU emulada debe realizar una emulación de código a nivel de procesador, es decir, debe ejecutar directamente el código malicioso, que, por lo tanto, no debe ejecutarse en la CPU del hardware (es decir, la CPU host del sistema emulado). | X | | |
| 15. El sandboxing basado en la emulación del sistema completo debe ser capaz de detectar ataques de múltiples etapas donde el exploit se divide en múltiples objetos | X | | |
| 16. Las actualizaciones de sandbox deben ejecutarse en línea automatizadamente, sin intervención manual. | X | | |
| 17. La solución debe ser capaz de identificar amenazas en cualquier formato de archivo. Enumerar los tipos de archivos soportados | X | | |
| 18. La solución debe integrar FIM (File Integrity Monitoring) ilimitado para servidores Windows y Linux, incluir sensores ilimitados. La características FIM se basa en alertas generadas por el Sistema Operativo Windows o Linux | X | | |
| 19. La solución debe proveer funciones de NTA (Network Traffic Analysis) sin licenciamiento adicional | X | | Se previno y fue subsanado |
| 20. La solución debe incluir tecnologías de Honeypots y deceptions | X | | |
| 21. La solución propuesta debe incluir capacidades de correlación avanzadas para detectar incidentes como: Ataques DDoS, Ataques de virus, Escaneo de puertos, Inyección de SQL, Ataques de Fuerza Bruta | X | | |
| 22. Ejecutar análisis de registros basado en búsquedas y reportería | X | | |
| 23. Analizar y correlacionar eventos de seguridad | X | | |
| 24. Enviar alertas al personal respectivo basado en el nivel de criticidad del evento | X | | |
| 25. La solución debe incluir gestión de amenazas e incidentes basado en cumplimiento | X | | |
| 26. La solución propuesta debe ser capaz de soportar colección de logs basado en agentes y sin agentes (Agentless) | X | | |
| 27. La solución debe ser capaz de ejecutar monitoreo de servidores y de red de oficinas remotas | X | | |
| 28. La solución debe ser capaz de ejecutar monitoreo rendimiento de aplicaciones (APM) | X | | |
| 29. Capaz de realizar el seguimiento de los cambios mediante el monitoreo de actividades sospechosas, cambios en el rol del usuario, acceso no autorizado. | X | | |

| **FUNCIONES QUE REALIZAR POR LA SOLUCIÓN PARA PARA LA ORQUESTACIÓN AUTOMATIZACIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD (SOAR) Los ofertantes deberán detallar en su oferta si la solución cumple con las funciones siguientes:** | **CUMPLE** | **NO CUMPLE** | **OBSERVACIONES** |
|---|---|---|---|
| 30. La solución debe ser capaz de enmascarar información como contraseñas, datos sensibles antes de almacenar en su base de datos | X | | |
| 31. La solución debe ser capaz de ejecutar geolocalización de los ataques | X | | |
| 32. La solución debe monitorear automáticamente los eventos negativos conocidos y utilizar una correlación sofisticada a través de la búsqueda para encontrar patrones de riesgo conocidos, como ataques de fuerza bruta, fuga de datos e incluso fraude a nivel de aplicación. | X | | |
| 33. La solución debe ser capaz de detectar dispositivos comprometidos asociados con amenazas avanzadas e infecciones de malware | X | | |
| 34. La solución debe ser capaz de encontrar actividades y eventos asociados con ataques e infecciones residentes en la red | X | | |
| 35. La solución debe ser capaz de ayudar a los analistas de seguridad a realizar evaluaciones de compromiso e incumplimiento. | X | | |
| 36. Que admita registros de seguridad personalizados que realice la correlación sobre los registros en movimiento en la red | X | | |
| 37. La solución debe ser capaz de correlacionar información de los dispositivos con información de amenazas y vulnerabilidades | X | | |
| 38. La solución debe ejecutar la recopilación pasiva de información de los activos e información del flujo de red | X | | |
| 39. La solución debe proveer una vista de los datos almacenados en formato crudo | X | | |
| 40. La solución debe emitir alerta al detectar IP externa en lista negra por reputación de dominio o IP | X | | |
| 41. La solución debe incluir alertas predefinidos de acuerdo al nivel de severidad detectado | X | | |
| 42. La solución debe ser completamente personalizable cuando se crea una alerta o alarma para eventos de alto riesgo | X | | |
| 43. La solución debe proporcionar visibilidad de red con información que contenga niveles de criticidad de los eventos, payloads, información de sesión, errores, DNS, etc. | X | | |
| 44. La solución debe proporcionar aplicaciones, utilidades y complementos predefinidos que brinden capacidades que van desde el monitoreo de la seguridad y la gestión avanzada de amenazas, sin necesidad de crear vistas especiales o casos de uso especifico | X | | |
| 45. La solución propuesta debe ser capaz de capturar eventos capturados de nuevos dispositivos sin requerir leer los datos completos del trafico visualizado | X | | |
| 46. La solución propuesta debe ser capaz de proporcionar una función de búsqueda que admita búsquedas simples de patrones de estilo booleano, así como expresiones regulares complejas. | X | | |
| 47. La solución propuesta debe permitir al analista crear consultas utilizando el método de búsqueda combinada. Una sola consulta puede contener palabras clave, condiciones basadas en campos y expresiones regulares. | X | | |
| 48. La solución debe ser capaz de monitorear amenazas desconocidas o de día cero. | X | | |

| FUNCIONES QUE REALIZAR POR LA SOLUCIÓN PARA PARA LA ORQUESTACIÓN AUTOMATIZACIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD (SOAR) **Los ofertantes deberán detallar en su oferta si la solución cumple con las funciones siguientes:** | CUMPLE | NO CUMPLE | OBSERVACIONES |
|---|---|---|---|
| 49. La solución debe ser capaz de correlacionar e identificar problemas de rendimiento de la aplicación debido a incidentes de seguridad (por ejemplo, ataques DDOS, acceso no autorizado al sistema que causa problemas de rendimiento de la aplicación). | X | | |
| 50. La solución debe poder descubrir sistemas con capacidad limitada o inactivos | X | | |
| 51. La solución propuesta debe poder ingerir todos los datos (usuarios, aplicaciones) y ponerlos a disposición para su uso: monitoreo, alertas, investigación, búsqueda ad hoc | X | | |
| 52. La solución debe tener widget y dashboard personalizable | X | | |
| 53. La solución debe ser administrable vía Web GUI vía HTTPS | X | | |
| 54. La solución debe proporcionar flexibilidad para integrarse con portales y herramientas de informes de terceros. La solución se debe integrar con cualquier solución de seguridad de maneras diferentes a través de sus reenviadores de registros, conectores, transmisión de datos y API abiertas, por ejemplo: Firewall, solución antivirus, active directory. | X | | |
| 55. La solución debe usar algoritmos basados en aprendizaje automático. Proporcionar algunos casos de uso y evidencia de que la aplicación está utilizando algoritmos basados en aprendizaje automático | X | | |
| 56. La solución debe proporcionar el Módulo de inteligencia preempaquetado para el sistema de base de datos, como Informix, MYSQL, MySQL, DB2, Oracle | X | | |
| 57. La solución debe proporcionar agentes para Windows con Módulo de inteligencia, Dashboard y reportería | X | | |
| 58. La solución debe configurarse para implementarse en el entorno de almacenamiento SAN del cliente existente. Que no requiera bases de datos adicionales para administración y reporteria | X | | |
| 59. La solución debe venir con la integración con al menos cinco tecnologías de inteligencia de amenazas de código abierto. | X | | |
| 60. La solución debe tener una consola de administración primaria compuesta de indexador y dashboard | X | | |
| 61. Posibilidad de implementar solución en alta disponibilidad | X | | |
| 62. La solución debe proveer visibilidad total de Ataques Avanzados (ATP) vía red, web o clientes | X | | |
| 63. La solución debe proporcionar capacidad de detección no basado en firma, sino en anomalías de trafico de red y comportamiento sospechoso | X | | |
| 64. La solución debe ser capaz de notificar eventos vía XML, JSON o formatos de texto como correo, envío de mensajes, etc. | X | | |
| 65. La solución debe enviar información de eventos vía SNMP | X | | |
| 66. La solución debe poder clasificar la severidad del incidente adjunto a las Alertas. | X | | |
| 67. La solución debe admitir el modo de bloqueo en línea (no el restablecimiento de TCP) | X | | |
| 68. La solución debe soportar integración con herramientas de análisis forense | X | | |
| 69. La solución debe soportar la detección de no menos 2000 dispositivos de red | X | | |
| 70. La solución debe tener la capacidad de reconocer eventos como parte de un flujo de trabajo. | X | | |

| FUNCIONES QUE REALIZAR POR LA SOLUCIÓN PARA PARA LA ORQUESTACIÓN AUTOMATIZACIÓN Y RESPUESTA A INCIDENTES DE SEGURIDAD (SOAR) **Los ofertantes deberán detallar en su oferta si la solución cumple con las funciones siguientes:** | CUMPLE | NO CUMPLE | OBSERVACIONES |
|---|---|---|---|
| 71. La solución debe ser capaz de reportar intentos de robo de información de parte de los usuarios | X | | |
| 72. La solución debe tener la capacidad de integrarse con Active Directory para identificación de usuarios | X | | |
| 73. La solución debe detectar amenazas de cualquier tipo de sistema operativo | X | | |
| 74. La solución debe tener la capacidad de instalar sensores en ambiente virtual | X | | |
| 75. La solución debe ser capaz de soportar interfaces de red de 1Gbps, 10 Gbps fibra y cobre | X | | |
| 76. La solución debe ser capaz de proveer correlación de eventos a través de varias fuentes de datos como Syslog, SNMP, o integraciones con terceros | X | | |
| 77. La solución debe proporcionar actualizaciones de inteligencia de amenazas de las plataformas de forma centralizada | X | | |
| 78. La solución debe proporcionar análisis en profundidad e informes sobre las tendencias de los actores de amenazas | X | | |
| 79. La solución debe proporcionar análisis en demanda de direcciones IPs y dominios. | X | | |
| 80. El motor de análisis debe ser capaz de revelar las técnicas de evasión utilizadas por el malware, como los bucles de detención y las comprobaciones ambientales; | X | | |
| 81. La licencia debe basarse en la cantidad de datos en tamaño de GIGABYTES (GB) que se envían a SIEM cada día. | X | | |
| 82. Debe permitir configurar acciones automatizadas hacia los diferentes dispositivos de seguridad de la red existentes, sin necesidad de adquirir una solución adicional para ejecutar la acción de bloqueo de sesiones o trafico sospechoso | X | | |

Con base a la evaluación técnica realizada, la unidad solicitante, determinó que el ofertante TRUST NETWORK, S.A. DE C.V., cumplió con la totalidad de las especificaciones técnicas requeridas en dicha evaluación por lo que se recomendó considerarla elegible para continuar con la negociación en la Bolsa en dicho ítem;

**VIII)** Que el 16 de abril de 2021, se realizó la rueda de negociación de la oferta de compra N° 329/2020, obteniendo el siguiente resultado:

| DESCRIPCIÓN DEL SERVICIO | PRECIO DE CALCE SIN IVA | PRECIO TOTAL DE CIERRE SIN IVA |
|---|---|---|
| SERVICIOS DE RENOVACIÓN DE SUSCRIPCIÓN DE LA SOLUCIÓN ANTISPAM Y FILTRADO DE MENSAJES DE CORREO ELECTRÓNICO ENTRANTE Y SALIENTE INSTITUCIONAL | $ 67,000.00 | $ 75,710.00 |
| **TOTAL** | | **$ 75,710.00** |

| NO. DE CONTRATO | DESCRIPCIÓN | PROVEEDOR | MONTO NEGOCIADO SIN IVA |
|---|---|---|---|
| 27874 | ÍTEMS # 1 | | $ 67,000.00 |
| MONTO CON IVA | | | $ 75,710.00 |
| TOTAL COMISIÓN BOLPROS (1%) MAS IVA INCLUIDO | | | $ 757.10 |
| MONTO TOTAL CONTRATADO DEL PROCESO | | | $ 76,467.10 |
| MONTO DE ASIGNACIÓN PRESUPUESTARIA CON IVA INCLUIDO | | | $ 79,600.00 |
| MONTO DE DIFERENCIA (AHORRO 3.93%) | | | $ 3,132.90 |

**IX)** Que el expositor de conformidad a lo dispuesto por los artículos 2 letra e), 2 de la Ley de Bolsas de Productos y Servicios; y 10 Requisitos de Constitución de las Bolsas; Convenio por Servicios de Negociación por Cuenta del Estado suscrito entre el CNR y BOLPROS, de fecha 22 de octubre de 2020, Reglamento General de la Bolsa, Instructivos de la Bolsa y conforme a lo instruido en el acuerdo de Consejo Directivo N° 37-CNR/2021, expedido en fecha 11 de febrero de 2021, ha solicitado al Consejo Directivo: I) darse por recibido del informe sobre los resultados del proceso referente a los ""Servicios de renovación de suscripción de la solución para la orquestación, automatización y respuesta a incidentes de seguridad (SOAR) y de la solución antispam y filtrado de mensajes de correo electrónico, entrante y saliente institucional, año 2021", desarrollado por medio de la bolsa, con la Oferta de Compra N° 329, según Acuerdo de Consejo Directivo N° 37-CNR/2021, de fecha 12 de noviembre de 2020, contratado con el proveedor TRUST NETWORK, S.A. DE C.V., – MULTISERVICIOS BURSÁTILES, S.A. por un monto total de hasta USD$ 75,710.00 con IVA; y una comisión bursátil del 1% más IVA equivalente a USD$ 757.10, sumando un total de hasta USD$ 76,467.10 con IVA y comisión de BOLPROS incluida, para el plazo de doce meses a partir del cierre de la negociación y contratación, es decir, para el período comprendido a partir del 16 de abril de 2021 al 16 de abril del 2022.

**Por tanto,** en uso de sus atribuciones legales, de conformidad a las razones expresadas y con base en lo dispuesto a las disposiciones legales antes citadas, el Consejo Directivo

**X)** **ACUERDA: I) Darse** por recibido del informe sobre los resultados del proceso referente a los "Servicios de renovación de suscripción de la solución para la orquestación, automatización y respuesta a incidentes de seguridad (SOAR) y de la solución antispam y filtrado de mensajes de correo electrónico, entrante y saliente institucional, año 2021", desarrollado por medio de la bolsa, con la Oferta de Compra N° 329, según Acuerdo de Consejo Directivo N° 37-CNR/2021, de fecha 12 de noviembre de 2020, contratado con el proveedor TRUST NETWORK, S.A. DE C.V., – MULTISERVICIOS BURSÁTILES, S.A. por un monto total de hasta USD$ 75,710.00 con

IVA; y una comisión bursátil del 1% más IVA equivalente a USD$ 757.10, sumando un total de hasta USD$ 76,467.10 con IVA y comisión de BOLPROS incluida, para el plazo de doce meses a partir del cierre de la negociación y contratación, es decir, para el período comprendido a partir del 16 de abril de 2021 al 16 de abril del 2022. **II) Comuníquese.** Expedido en San Salvador, veinticuatro de agosto de dos mil veintiuno.


Jorge Camilo Trigueros Guevara
Secretario del Consejo Directivo