INFORME DE EVALUACIÓN Y RECOMENDACIÓN DE ADJUDICACIÓN A LA CONVOCATORIA DE MENOR CUANTIA NACIONAL N° 06/2024
"RENOVACION DE LICENCIAS ANTIVIRUS"
ID 449.290
"EVALUACIÓN BASADA EN PRECIO"

1. INTRODUCCION:

En la ciudad de Asunción, Capital de la República del Paraguay a los veintiún días del mes de noviembre del año dos mil veinticuatro, siendo las 10:00 horas, en la dependencia de la Dirección General de Tecnologías de la Información del Instituto Nacional de Desarrollo Rural y de la Tierra, sito en Tacuary Nº 276 e/ Mariscal Estigarribia se reúnen los miembros del Comité de Evaluación de Ofertas, de la convocatoria a Licitación por Menor Cuantía Nacional Nº 06/2024 "Renovación de Licencias Antivirus". Dicho procedimiento se efectúa conforme a las disposiciones contenidas en la Ley N° 7021/2022 de "De Suministro y Contrataciones Públicas" reglamentada por el Decreto Nº 2264/2024, y la Resolución Presidencia Nº 1974/2024 "Que Aprueba el Pliego de Bases y Condiciones, Autoriza el Llamado y Crea e Integra el Comité de Apertura y Evaluación, Respectivamente para la convocatoria a Licitación por Menor Cuantía Nacional Nº 06/2024 "Renovación de Licencias Antivirus" ID 449.290".

Para tal efecto, fueron designados los siguientes funcionarios del INDERT:

- Sr. Peter Poka, Jefe de Administración de Base de Datos
- Sr. Juan Fernández, Director de Sistemas Informáticos.-
- C.P. Pablo Ariel Velázquez, Jefe del Dpto. de Análisis y Evaluación de Contabilidad.-
- Abg. Mariel Contrera Caballero, Asesora Jurídica.-

2. ACTA DE APERTURA

En fecha 07 de noviembre del año 2024, en las oficinas de la Unidad Operativa de Contrataciones del Instituto Nacional de Desarrollo Rural y de la Tierra, se procedió al acto de apertura de sobres de ofertas económicas, cumplido los requisitos exigidos en la Ley N° 7021/22 y su Decreto Reglamentario N° 2264/24, y habiéndose puesto el presente llamado a través del Sistema de Información de las Contrataciones Públicas (SICP) Portal de Contrataciones Públicas para que cualquier potencial oferente que tenga interés y que pueda satisfacer los requisitos establecidos en los Términos de Referencia acuda a presentar su oferta.

Presentaron Ofertas las firmas:

- **CORPORATION SEKIURA S.A.C.E.I.**

3. DISPONIBILIDAD PRESUPUESTARIA.

Los rubros para esta Contratación se hallan previstos en la partida **579 – Activos Intangibles asignado al INDERT dentro del Presupuesto General de la Nación con Fuente de Financiamiento 30 Recursos Institucionales para el Ejercicio Fiscal 2024.** Cuenta con el correspondiente Certificado de Disponibilidad Presupuestaria N° 75/2024, emitida por del Dpto. de Presupuesto y aprobada por la Gerencia de Administración y Finanzas del INDERT, por el monto total de **Gs. 333.807.342 (Guaraníes Trescientos treinta y tres millones, ochocientos siete mil, trescientos cuarenta y dos).**

Abog. Mariel Contrera C.
Asesora Jurídica
INDERT

Juan Fernández
Director
Dirección de Sistemas Informáticos
INDERT

Peter Poka

C.P Pablo A. Velazquez
Jefe Dpto. de Análisis y Evaluación
INDERT

4. VERIFICACIÓN DEL CUMPLIMIENTO DE LOS REQUISITOS DE CARÁCTER SUSTANCIAL.

Conforme a los métodos de evaluación y criterios establecidos en los Artículo 75 del Decreto N° 2264/24, que reglamenta la Ley N° 7021/22 "De Suministro y Contrataciones Públicas" se procede a la evaluación de las ofertas y se verifica el cumplimiento de las mismas respecto al suministro de la documentación básica de carácter sustancial.

Pasamos a efectuar el análisis de las documentaciones de la propuesta de conformidad a la disposición contenida en el Art. 79. *Documentos Sustanciales* del Decreto N° 2264/24 que reglamenta la Ley N° 7021/22 de Contrataciones Públicas, con el siguiente resultado:

Oferentes	Documentos de Carácter Sustancial			
	El formulario de oferta y la lista de precios generada electrónicamente a través del SICP, debidamente llenados y firmados.	La Garantía de Mantenimiento de Oferta debidamente extendida	Documentos que acrediten la existencia del Oferente	Los documentos que demuestren las facultades del firmante de la oferta, para comprometer al oferente
CORPORATION SEKIURA S.A.E.C.I.	Cumple	Cumple	Cumple	Cumple

5. TABLA COMPARATIVA DE PRECIOS DE LAS OFERTAS AJUSTADA POR ERRORES ARITMÉTICOS:

De conformidad a la disposición contenida en el del Art. 75 del Decreto N° 2264/24, se ha procedido a la verificación de las planillas de precio presentadas por las firmas que han cumplido con la documentación de carácter sustancial, resultando que *ninguna de ellas presenta errores aritméticos.* A continuación, se procede a la verificación de las ofertas económica presentadas por los oferentes, conforme al cuadro que se detalla a continuación:

ANEXO I - CUADRO COMPARATIVO LICITACIÓN DE MENOR CUANTÍA N° 06/2024 RENOVACION DE LICENCIAS ANTIVIRUS RENOVACION DE LICENCIAS						
SEKIURA S.A.C.E.I.						
Ítem	Descripción del Bien	CANT.	Unidad de Medida	Present.	Precio Unitario	Precio Total IVA Incluido
1	Renovación de Licencias Kaspersky Endpoint Security for Business con servicio de Instalación y Soporte por 1 año.-	475	Unidad	Unidad	464.000	220.400.000
2	Renovación de Licencias Kaspersky Security for Mail Server con servicio de Instalación y Soporte por 1 año.-	200	Unidad	Unidad	244.000	48.800.000
3	Renovación de Licencias – Protección de copias de Seguridad – Barracuda 490 con licenciaciamiento por 1 año.-	1	Unidad	Unidad	49.000.000	49.000.000
4	Renovación de Licencias – Protección de Firewall perimetral – WatchGuard Firebox M370 con licenciamiento por 1 año.	4	Unidad	Unidad	14.950.000	14.950.000
					Total	**333.150.000**

5.1 APLICACIÓN DE MARGEN DE PREFERENCIA:

En el marco del presente proceso de contratación no se aplica el margen de preferencia, en consecuencia de que las propuestas no han presentado productos de procedencia nacional.-

6. EVALUACIÓN Y RECOMENDACIÓN POR EL SISTEMA DE EVALUACIÓN POR EL TOTAL:

Conforme lo establece el Art. 75 del Decreto Reglamentario N° 2264/24 de la Ley N° 7021/22, que dice: *"...Se seleccionará provisoriamente a la oferta con el menor precio, la que será analizada en detalle para verificar su cumplimiento con otros requisitos de la contratación"*, se toman las ofertas presentadas por las firmas detalladas abajo y que son analizadas en detalle:

A continuación, este comité de evaluación, en cumplimiento a los requisitos establecidos en el Pliego de Bases y Condiciones, toma la única oferta presentada por la firma **CORPORATION SEKIURA S.A.E.C.I.** por la suma de **Gs. 333.150.000** (**Guaraníes, Trescientos treinta y tres millones, ciento cincuenta mil**) que es analizada en detalle:

Abog. Mariel Contrera C.
Asesora Jurídica
INDERT

Juan Fernández
Director
Dirección de Sistemas Informáticos
INDERT

C.P Pablo A. Velázquez
Jefe Dpto. de Análisis y Evaluación
INDERT

7. ANÁLISIS DE PRECIOS OFERTADOS.

Se realiza el análisis de los precios ofertados por la firma CORPORATION SEKIURA S.A.E.C.I., con los resultados consignados de las condiciones descriptas en la Resolución DNCP Nº 454/2024, todos los precios ofertados se encuentran en el rango permitido de acuerdo al siguiente cuadro:

ANEXO II - ANALISIS DE PRECIOS OFERTADOS							
LICITACIÓN DE MENOR CUANTÍA N° 06/2024 RENOVACION DE LICENCIAS ANTIVIRUS							
Ítem	DESCRIPCIÓN	Cant.	SEKIURA S.A.E.C.I.				
			Precio Unitario	Precio Ref.	>15%	<25%	Resultado
1	Renovación de Licencias Kaspersky Endpoint Security for Business con servicio de Instalación y Soporte por 1 año.-	475	464.000	450.000	517.500	337.500	ESTA EN EL RANGO
2	Renovación de Licencias Kaspersky Security for Mail Server con servicio de Instalación y Soporte por 1 año.-	200	244.000	235.000	270.250	176.250	ESTA EN EL RANGO
3	Renovación de Licencias – Protección de copias de Seguridad – Barracuda 490 con licenciaciamiento por 1 año.-	1	49.000.000	49.500.000	56.925.000	37.125.000	ESTA EN EL RANGO
4	Renovación de Licencias – Protección de Firewall perimetral – WatchGuard Firebox M370 con licenciamiento por 1 año.	1	14.950.000	15.000.000	17.250.000	11.250.000	ESTA EN EL RANGO

8. VERIFICACIÓN DE DOCUMENTOS CONFORME AL PLIEGO DE BASES Y CONDICIONES.

REQUISITOS DOCUMENTALES PARA EVALUACIÓN DE LAS CONDICIONES DE PARTICIPACIÓN.	
	SEKIURA S.A.C.E.I.
Certificado de Cumplimiento con la Seguridad Social (**)	Cumple
Certificado de Producto y Empleo Nacional, emitido por el MIC, en caso de contar. (**)	No Aplica
Certificado de Cumplimiento Tributario. (**)	Cumple
Patente comercial del municipio en donde esté asentado el establecimiento del oferente. (**)	Cumple
Declaración Jurada de "Declaración de Personas", de conformidad con el formulario estándar - Sección Formularios (**)	Cumple

Los documentos indicados con doble asterisco (**) deberán estar vigentes a la fecha y hora tope de presentación de ofertas como lo establece el Pliego de Bases y Condiciones.-

DOCUMENTOS LEGALES PARA OFERENTES INDIVIDUALES. PERSONAS JURÍDICAS.	
	SEKIURA S.A.C.E.I.
Fotocopia simple de los documentos que acrediten la existencia legal de la persona jurídica tales como la Escritura Pública de Constitución y protocolización de los Estatutos Sociales. Los estatutos deberán estar inscriptos en la Sección Personas Jurídicas de la Dirección de Registros Públicos. (*)	Cumple
Constancia de inscripción en el Registro Único de Contribuyentes. (*)	Cumple
Fotocopia simple de los documentos de identidad de los representantes o apoderados de la sociedad. (*)	Cumple
Fotocopia simple de los documentos que acrediten las facultades del firmante de la oferta para comprometer al oferente. Estos documentos pueden consistir en: un poder suficiente otorgado por Escritura Pública (no es necesario que esté inscripto en el Registro de Poderes); o los documentos societarios que justifiquen la representación del firmante, tales como las actas de asamblea y de directorio en el caso de las sociedades anónimas. (*)	Cumple

AUTORIZACIÓN DEL FABRICANTE	
	SEKIURA S.A.C.E.I.
Autorización del Fabricante, Representante o Distribuidor	Cumple

EXPERIENCIA REQUERIDA	SEKIURA S.A.C.E.I.
Demostrar la experiencia en ser proveedor de los bienes solicitados en el presente llamado: **Ítem 1 - Renovación de Licencias Kaspersky Endpoint Security for Business Select con Servicio de Instalación y Soporte 1 año** **Ítem 2 - Renovación de Licencias Kaspersky Security for Mail Server(AntiSpan) (Con Servicio de Instalación y Soporte)** **Ítem 3 - Renovación de Licencias Protección de copias de seguridadBarracuda Backup 490 con licenciamiento 1año** **Ítem 4 - Renovación de Licencias Protección de Firewall perimetral WatchGuard Firebox M370 con licenciamiento 1año** con contrato o con facturaciones de venta y/o recepciones finales por un monto equivalente al 50 % (CINCUENTA) como mínimo del monto total ofertado en la presente licitación, de los: 2021, 2022 y 2023.-	Cumple
REQUISITOS DOCUMENTALES PARA LA EVALUACIÓN DE LA EXPERIENCIA	**SEKIURA S.A.C.E.I.**
Copia de facturaciones y/o recepciones finales que avalen la experiencia requerida de los años 2021, 2022 y 2023.	Presento
Copia de contratos de los años 2021, 2022 y 2023, con certificado de cumplimiento satisfactorio del contrato.-	Presento

C.P Pablo A. Velázquez
Jefe Dpto. de Análisis y Evaluación
ANDE

Juan Fernández
Director
Dirección de Sistemas Informáticos
ANDE

Abog. [illegible]
Asesoría Jurídica
ANDE

9. VERIFICACIÓN DE LA CAPACIDAD TÉCNICA SEGÚN EL PLIEGO DE BASES Y CONDICIONES:

Se procede a la verificación conforme al siguiente cuadro detallado a continuación:

El oferente deberá proporcionar evidencia documentada que demuestre su cumplimiento con los siguientes requisitos de capacidad técnica:	**SEKIURA S.A.C.E.I.**
Planilla de Cumplimiento de los Bienes ofertados con las Especificaciones Técnicas: debidamente completada y firmada conforme al formato establecido en la Sección de Suministros requeridos - Especificaciones Técnicas. Deberán detallar el número de página del catálogo donde se cumple con el requerimiento (conforme catálogo y lo declarado en planilla); la falta de información clara y precisa será motivo de descalificación.	Cumple
El oferente deberá presentar catálogos, anexos técnicos, manual de software y otras documentaciones en español o Ingles que contengan toda la información necesaria del bien ofertado, deberán contener mínimamente, imagen y los datos de las Especificaciones Técnicas ofertadas, debe indicar el sitio oficial del fabricante para su verificación. La falta de información clara y precisa será motivo de descalificación.	Cumple
El oferente deberá presentar en carácter de Declaración Jurada el listado de las soluciones ofertadas. Se deberá indicar el sitio oficial del fabricante para la verificación de las soluciones a ser adquiridas, no serán aceptadas otras formas de verificación. Aplica para todos los ítems.	Cumple
Carta de Autorización del fabricante dirigido a la institución y con referencia al proceso. No sean aceptadas cartas genéricas. (Aplica para todos los ítems).	Cumple
El oferente deberá acreditar la Certificación ISO 27001/2013 o superior con alcance en Servicio de Soporte técnico y de seguridad de software del área de Tecnología para el Sector Publico (no serán aceptadas certificaciones genéricas), la certificación superior debe basarse en los mismos criterios que solicita o certifica la norma ISO 27001/2013 con respecto a la gestión de la seguridad.-	Cumple
Requisitos documentales para evaluar el criterio de capacidad técnica	**SEKIURA S.A.C.E.I.**
Planilla de Cumplimiento de los Bienes/Software ofertados con las Especificaciones Técnicas, debidamente completada y firmada.	Presento
Catálogos, anexos técnicos, manual de software y otras documentaciones en español o inglés que respalde el cumplimiento con lo solicitado, indicando el ítem al cual corresponde.	Presento
Carta de Autorización del fabricante	Presento
El oferente deberá acreditar la Certificación ISO 27001/2013 o superior con alcance en Servicio de Soporte técnico y de seguridad de software del área de Tecnología para el Sector Publico, la certificación superior debe basarse en los mismos criterios que solicita o certifica la norma ISO 27001/2013 con respecto a la gestión de la seguridad, confidencialidad e integridad de los datos	Presento

10. VERIFICACIÓN DEL CUMPLIMIENTO AL ARTÍCULO 21 DE LA LEY 7021/2022 CONFORME A LA RESOLUCIÓN DNCP N° 4401/23.

Por otra parte el Comité de Evaluación mediante Nota de fecha 18 de Noviembre de 2024, ha solicitado al Dpto. de Liquidación de Salarios y Otros dependiente de la Dirección General de Gestión y Desarrollo de Personas del INDERT, verificar en los registros del personal del INDERT y en la BASE DE DATOS del Sistema Integrado de Administración de Recursos Humanos (SINARH) para detectar si el oferente o sus representantes se hallan comprometidos en los presupuestos, en cumplimento del Art. 21 de la Ley 7021/2022 y la Resolución DNCP N° 4401/23 :

Nº	EMPRESA	NOMBRES Y APELLIDOS	CÉDULA DE IDENTIDAD	CARGO
1	SEKIURA S.A.C.E.I.	NELIDA RAFAELA APONTE DE FISCHER	397.359	REPRESENTANTE LEGAL
2		INGRID FISCHER APONTE	4.204.194	ACCIONISTA

El Departamento de Liquidación de Salarios y Otros dependientes de la Dirección General de Gestión y Desarrollo de Personas del INDERT, mediante Nota de fecha 21 de Noviembre de 2024, informa a este Comité que las citadas personas no se registran en los registros del personal del INDERT ni en la Base de Datos del Sistema Integrado de Administración de Recursos Humanos (SINARH), el citado documento forma parte del presente informe.

Abog. Mariel Contrera C.
Asesora Jurídica

Juan Fernández
Director
Dirección de Sistemas Informáticos

C.P Pablo A. Velázquez
Jefe Dpto. de Análisis y Evaluación

11. VERIFICACIÓN DE LAS ESPECIFICACIONES TÉCNICAS CONFORME AL PLIEGO DE BASES Y CONDICIONES:

SUMINISTROS REQUERIDOS

Ítem N° 1 Renovación de Licencias – Kaspersky Endpoint Security for Business Select con Servicio de Instalación y Soporte – 1 año

Nº	Especificaciones Técnicas	Mínimo Exigido	SEKIURA S.A.C.E.I. Cumple con las especificaciones requeridas (si/no)
1.1	Se debe proveer una solución tecnológica que incluya una poderosa protección de endpoints basada en IA, controles de seguridad flexibles y características de EDR incorporadas.	EXIGIDO	CUMPLE
1.2	La solución debe contar con una consola fácil de usar, opciones de implementación en la nube y on-premises, así como también una variedad de funciones que simplifiquen la vida del usuario, reduciendo la complejidad y aumentando la eficiencia.	EXIGIDO	CUMPLE
1.3	La solución debe proteger endpoints y servers, sean estos Windows, Linux, macOS, así como también dispositivos móviles iOS y Android.	EXIGIDO	CUMPLE
1.4	La solución debe disponer de una única licencia que debe permitir el uso de la consola nube u on-premise, como así también de todos los endpoints y servers que disponga la organización, independientemente del sistema operativo del dispositivo en cuestión.	EXIGIDO	CUMPLE
1.5	La solución debe permitir la implementación de puntos de distribución en diferentes segmentos de red o ubicaciones geográficas de la organización quepermita la distribución de actualizaciones, sondeo de red, instalación remota de aplicaciones, obtención de información sobre equipos de un grupo de administración, y/o difusión de dominio, entre otras.	EXIGIDO	CUMPLE
1.6	La solución debe incluir una infraestructura de servicios en la nube que brinde acceso a la base de conocimientos del fabricante, ofreciendo un recurso en línea que permita conocer la reputación de los archivos, los recursos web y el software, garantizando respuestas más rápidas ante nuevas amenazas, mejorando el rendimiento de algunos componentes de protección y reduciendo el riesgo probable de que se produzcan falsos positivos	EXIGIDO	CUMPLE
1.7	La solución debe contar con la capacidad de eliminar remotamente cualquier solución antivirus (propia o de terceros) que esté presente en los endpoints y servidores, sin la necesidad de la contraseña de remoción del actual antivirus	EXIGIDO	CUMPLE
1.8	La solución debe disponer de la capacidad de instalar remotamente la solución de antivirus en los endpoints y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory;	EXIGIDO	CUMPLE
1.9	La solución debe contar con la capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto;	EXIGIDO	CUMPLE
1.10	La solución debe disponer de la capacidad de importar la estructura de Active Directory para encontrar máquinas;	EXIGIDO	CUMPLE
1.11	La solución debe contar con la capacidad de monitorear diferentes subnets de red con el objetivo de encontrar máquinas nuevas para que sean agregadas a la protección;	EXIGIDO	CUMPLE
1.12	La solución debe disponer de la capacidad de, al detectar máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antivirus instalado. En caso de no tenerlo, debe instalar el antivirus automáticamente;	EXIGIDO	CUMPLE

Abog. Mariel Contrera
Asesora Jurídica

Juan Fernández
Director
Dirección de Sistemas Informáticos
INDERT

Pedro Polka.

C.P Pablo L. Velázquez
Jefe Dpto. de Análisis y Evaluación
INDERT

Ítem N° 2 Renovación de Licencias Kaspersky Security for Mail Server(AntiSpan) (Con Servicio de Instalación y Soporte)

Nº	Especificaciones Técnicas	Mínimo Exigido	SEKIURA S.A.C.E.I. Cumple con las especificaciones requeridas (si/no)
2.1	La solución debe combinar protección basada en firmas, análisis heurístico y de comportamiento, junto con tecnologías asistidas por la nube para proteger los endpoints contra amenazas de malware conocidas, desconocidas y avanzadas.	EXIGIDO	CUMPLE
2.2	La solución debe permitir habilitar la protección con contraseña con el fin de restringir el acceso de los usuarios a la solución en la estación de trabajo según los permisos que se le otorgaron (por ejemplo, permiso para salir de la aplicación).	EXIGIDO	CUMPLE
2.3	La solución debe proporcionar mecanismos de autoprotección con el fin de evitar que otras aplicaciones realicen acciones que puedan interferir con el funcionamiento de la solución propuesta	EXIGIDO	CUMPLE
2.4	La solución debe permitir realizar un análisis personalizado para cualquiera de los siguientes objetos: Memoria del sistema, Objetos cargados en el inicio del sistema operativo, Copia de seguridad del sistema operativo, Buzón de correo de Microsoft Outlook, Unidades de disco duro, Unidades extraíbles y unidades de red o Cualquier archivo seleccionado	EXIGIDO	CUMPLE
2.5	La solución debe permitir realizar un análisis en segundo plano de manera que la aplicación no le muestre ninguna notificación al usuario y que tenga menos impacto en los recursos del equipo, para cualquiera de los siguientes objetos: objetos de inicio, el sector de arranque, la memoria del sistema y la partición del sistema	EXIGIDO	CUMPLE
2.6	La solución debe permitir establecer una programación para el análisis, de manera que se pueda realizar de forma manual o según programación	EXIGIDO	CUMPLE
2.7	La solución debe permitir analizar archivos compuestos de formatos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos	EXIGIDO	CUMPLE
2.8	La solución debe permitir analizar archivos protegidos con contraseña	EXIGIDO	CUMPLE
2.9	La solución debe incorporar un componente de protección frente a amenazas web que permita evitar la descarga de archivos maliciosos de Internet y también bloquee sitios web maliciosos y de phishing	EXIGIDO	CUMPLE
2.10	La solución debe analizar tráfico HTTP, HTTPS y FTP	EXIGIDO	CUMPLE
2.11	La solución debe bloquear el tráfico HTTP que no cumple con los estándares RFC	EXIGIDO	CUMPLE
2.12	La solución debe incluir un componente de protección frente a amenazas en el correo que permita analizar los archivos adjuntos de mensajes de correo electrónico entrantes y salientes en busca de virus y otra amenaza	EXIGIDO	CUMPLE
2.13	La solución de protección frente a amenazas en el correo debe ser compatible con POP3, SMTP, IMAP y NNTP	EXIGIDO	CUMPLE
2.14	La solución de protección frente a amenazas en el correo debe intentar desinfectar un objeto infectado en un mensaje entrante o saliente. Si el objeto no se puede desinfectar, el componente de protección en el correo deberá eliminar el objeto infectado y añadir información sobre la acción realizada al asunto del mensaje, por ejemplo: [Se ha procesado el mensaje] <asunto del mensaje	EXIGIDO	CUMPLE
2.15	La solución debe combinar protección basada en firmas, análisis heurístico y de comportamiento, junto con tecnologías asistidas por la nube para proteger los endpoints contra amenazas de malware conocidas, desconocidas y avanzadas.	EXIGIDO	CUMPLE
2.16	La solución debe bloquear la conexión de red con el equipo atacante	EXIGIDO	CUMPLE
2.17	La solución debe incluir una base de datos que ofrezca descripciones de los tipos de ataques de red actualmente conocidos y los modos para contrarrestarlos	EXIGIDO	CUMPLE
2.18	La solución debe bloquear el equipo que realiza el ataque y restringir el envío de paquetes de red durante un periodo determinado de al menos una hora.	EXIGIDO	CUMPLE
2.19	La solución debe permitir seleccionar el protocolo y el puerto que se van a usar para la comunicación y permitir actividades de red específicas	EXIGIDO	CUMPLE

Abog. Mariel Contrera C
Asesora Jurídica
ANDERT

Juan Fernández
Director
Dirección de Sistemas Informáticos
ANDERT

C.P. Pablo A. Velázquez
Jefe Dpto. de Análisis y Evaluación
ANDERT

2.20	La solución debe permitir activar y administrar la protección contra los siguientes tipos de ataques a la red, mínimamente: Inundación de red (flooding) ataques de tipo "Port scan", Ataques de spoofing de MAC	EXIGIDO	CUMPLE
2.21	La solución debe incluir un componente de Firewall de escritorio que bloquee las conexiones no autorizadas al equipo mientras se trabaja en Internet o en la red local.	EXIGIDO	CUMPLE
2.22	El componente de firewall de escritorio debe controlar la actividad de red de las aplicaciones en el equipo	EXIGIDO	CUMPLE
2.23	El componente de firewall de escritorio debe proporcionar protección del equipo con la ayuda de bases de datos antivirus, el servicio de inteligencia global en la nube y reglas de red predefinidas	EXIGIDO	CUMPLE
2.24	El componente de firewall de escritorio debe incluir un componente prevención de intrusiones en el host que proporcione acceso controlado de las aplicaciones a los recursos, procesos y datos personales del sistema operativo mediante el uso de derechos de aplicación	EXIGIDO	CUMPLE
2.25	El componente de firewall de escritorio debe controlar la actividad de la red sobre el protocolo seleccionado: TCP, UDP, ICMP, ICMPv6, IGMP y GRE	EXIGIDO	CUMPLE
2.26	El componente de firewall de escritorio debe permitir seleccionar los adaptadores de red que pueden enviar o recibir paquetes de red	EXIGIDO	CUMPLE
2.27	El componente de firewall de escritorio debe permitir restringir el control de los paquetes de red según su período de vida (TTL)	EXIGIDO	CUMPLE
2.28	El componente de firewall de escritorio debe, de forma predeterminada, crear un conjunto de reglas de red para cada grupo de aplicaciones que la solución detecta en el equipo	EXIGIDO	CUMPLE
2.29	La solución debe incluir un componente de prevención de ataques a nivel de USB impide que dispositivos USB infectados que emulan un teclado se conecten al equipo	EXIGIDO	CUMPLE
2.30	El componente de prevención de ataques a nivel de USB debe permitir que los dispositivos USB que el sistema operativo identifique como teclados y que estén conectados al equipo antes de instalar el componente se consideren autorizados después de la instalación del componente	EXIGIDO	CUMPLE
2.31	El componente de prevención de ataques a nivel de USB debe bloquear automáticamente el dispositivo USB si el código de autorización se introduce incorrectamente un número de veces especificado	EXIGIDO	CUMPLE
2.32	El componente de prevención de ataques a nivel de USB debe bloquear automáticamente el dispositivo USB si el código de autorización se introduce incorrectamente un número de veces especificado	EXIGIDO	CUMPLE
2.33	El componente de prevención de ataques a nivel de USB debe permitir utilizar un teclado en pantalla para autorizar dispositivos USB que no permitan introducir caracteres aleatorios (p.ej., escáneres de códigos de barras)	EXIGIDO	CUMPLE
2.34	La solución debe incluir un componente de protección AMSI diseñado para ser compatible con Antimalware Scan Interface de Microsoft	EXIGIDO	CUMPLE
2.35	El componente de protección AMSI debe permitir configurar el análisis de protección AMSI para archivos compuestos, como archivos de almacenamiento, paquetes de distribución o archivos en formatos de Office	EXIGIDO	CUMPLE
2.36	La solución debe incluir un componente de prevención de exploits que permita detectar código de software diseñado para aprovechar vulnerabilidades en el equipo y, a través de estas, realizar acciones maliciosas o abusar de los privilegios de administración	EXIGIDO	CUMPLE
2.37	El componente de prevención de exploits debe incluir un mecanismo de protección de la memoria de procesos del sistema, de manera que la solución bloquee los procesos externos que intentan acceder a los procesos del sistema	EXIGIDO	CUMPLE
2.38	La solución debe incluir un componente de prevención de intrusiones en el host que evite que las aplicaciones realicen acciones que puedan resultar peligrosas para el sistema operativo	EXIGIDO	CUMPLE
2.39	El componente de prevención de intrusiones en el host debe controlar el funcionamiento de las aplicaciones mediante el uso de derechos de las aplicaciones	EXIGIDO	CUMPLE
2.40	Los derechos de las aplicaciones deben incluir los siguientes parámetros de acceso: ✓ 2.40.1. - Acceso a recursos del sistema operativo (por ejemplo, opciones de inicio automático y claves de registro) ✓ 2.40.2. - Acceso a datos personales (como archivos y aplicaciones)"	EXIGIDO	CUMPLE

Abog. Mariel Contrera C
Asesora Jurídica
INDERT

Director
Unidad de Sistemas Informáticos
INDERT

C.P Pablo A. Velázquez
Jefe Dpto. de Análisis y Evaluación
INDERT

2.41	El componente de prevención de intrusiones en el host debe activar la protección del acceso a audio y vídeo, de manera que se evite que los ciberdelincuentes puedan usar programas especiales para intentar obtener acceso a dispositivos que graban audio y vídeo (como micrófonos o cámaras web), controlando cuándo las aplicaciones reciben una transmisión de audio o vídeo y protege los datos contra la interceptación no autorizada	EXIGIDO	CUMPLE
2.42	La solución debe incluir un componente de motor de reparación que le permita revertir las acciones realizadas por aplicaciones maliciosas en el sistema operativo.	EXIGIDO	CUMPLE
2.43	"El componente de motor de reparación debe permitir anular la actividad de malware en el sistema operativo a los siguientes tipos de actividad de malware: ✓ 2.43.1. - Elimina los archivos ejecutables que el malware ha creado (en cualquier tipo de soporte, excepto unidades de red) ✓ 2.43.2. - Elimina los archivos ejecutables creados por programas en los que el malware se ha infiltrado ✓ 2.43.3. - Restaura los archivos que el malware ha modificado o eliminado ✓ 2.43.4. - Elimina las claves del registro que el malware ha creado ✓ 2.43.5. - No restaura las claves del registro que el malware ha modificado o eliminado ✓ 2.43.6. - Finaliza los procesos iniciados por el malware ✓ 2.43.7. - Finaliza los procesos en los que haya penetrado una aplicación maliciosa ✓ 2.43.8. - No reanuda procesos que el malware haya suspendido ✓ 2.439. - Bloquea la actividad de red del malware ✓ 2.43.10. - Bloquea la actividad de red de los procesos en los que el malware se ha infiltrado."	EXIGIDO	CUMPLE
2.44	La solución debe incluir un componente de control web que permita regular el acceso de los usuarios a los recursos web	EXIGIDO	CUMPLE
2.45	El componente de control web debe permitir supervisar tráfico HTTP y HTTPS	EXIGIDO	CUMPLE
2.46	"El componente de control web debe permitir configurar el acceso a los sitios web a través de estos criterios ✓ 2.46.1. - Categorías de sitios web ✓ 2.46.2. - Tipo de datos ✓ 2.46.3. - Direcciones individuales"	EXIGIDO	CUMPLE
2.47	El componente de control web debe permitir la creación de reglas de acceso a recursos web mediante el uso de filtros y acciones que la solución realiza cuando el usuario visita recursos web	EXIGIDO	CUMPLE
2.48	El componente de control web debe utilizar al menos los siguientes filtros: ✓ 2.48.1. - Filtrar por contenido y tipo de datos ✓ 2.48.2. - Filtrar por direcciones de recursos web ✓ 2.48.3. - Filtrar por nombres de usuarios y grupos de usuarios"	EXIGIDO	CUMPLE
2.49	El componente de control web debe permitir seleccionar alguna de las siguientes acciones: ✓ 2.49.1. - Permitir ✓ 2.49.2. - Bloquear ✓ 2.49.3. - Advertir"	EXIGIDO	CUMPLE
2.50	La solución debe incluir un componente de control de dispositivos que administre el acceso de los usuarios a dispositivos instalados o conectados al equipo (por ejemplo, discos duros, cámaras o módulos wifi), con el fin de proteger el equipo de infecciones cuando se conectan los dispositivos; y se evitan pérdidas o fugas de datos	EXIGIDO	CUMPLE
2.51	El componente de control de dispositivos debe controlar el acceso a los siguientes niveles: ✓ 2.51.1. - Tipo de dispositivo ✓ 2.51.2. - Bus de conexión ✓ 2.51.3. - Dispositivos de confianza"	EXIGIDO	CUMPLE
2.52	El componente de control de dispositivos debe permitir la creación de reglas de acceso que permitan ajustar la configuración que determina qué usuarios pueden usar dispositivos instalados en un equipo o conectados a él	EXIGIDO	CUMPLE

Abog. Mariel Contrera
Asesora Jurídica
INDERT

Juan Fernández
Director
Inspección de Sistemas Informáticos
INDERT

C.P Pablo M. Velázquez
Jefe Dpto. de Análisis y Evaluación
INDERT

10

2.53	El componente de control de dispositivos debe permitir crear reglas del acceso para los siguientes tipos de dispositivo, mínimamente: ✓ 2.53.1. - Discos duros ✓ 2.53.2. - Unidades extraíbles (incluidas las unidades flash USB) ✓ 2.53.3. - Disquetes ✓ 2.53.4. - Unidades de CD/DVD ✓ 2.53.5. - Dispositivos portátiles (MTP) ✓ 2.53.6. - Impresoras locales ✓ 2.53.7. - Impresoras de red ✓ 2.53.8. - Módems ✓ 2.53.9. - Unidades de cinta ✓ 2.53.10. - Dispositivos multifuncionales ✓ 2.53.11. - Lectores de tarjetas inteligentes ✓ 2.53.12. - Dispositivos Windows CE USB ActiveSync ✓ 3.52.13. - Adaptadores de red externos ✓ 3.52.14. - Bluetooth ✓ 3.52.15. - Cámaras y escáneres"	EXIGIDO	CUMPLE
2.54	El componente de control de dispositivos debe proporcionar funciones de Anti-Bridging con el fin de impedir establecer conexiones de red simultáneas en un equipo para prevenir la creación de puentes de red.	EXIGIDO	CUMPLE
2.55	La solución debe incluir un componente de control de aplicaciones que permita gestionar el inicio de aplicaciones en los equipos de los usuarios	EXIGIDO	CUMPLE
2.56	El componente de control de aplicaciones debe permitir crear categorías de aplicaciones que se quieren gestionar	EXIGIDO	CUMPLE
2.57	El componente de control de aplicaciones debe permitir crear reglas en la directiva para el grupo de administración	EXIGIDO	CUMPLE
2.58	El componente de control de aplicaciones debe poder funcionar en dos modos: ✓ 2.58.1. - Lista de rechazados. En este modo, el control de aplicaciones autoriza a todos los usuarios a que inicien todas las aplicaciones, excepto aquellas que se prohíben en las reglas de control de aplicaciones. ✓ 2.58.2. - Lista de permitidos: en este modo, el control de aplicaciones bloquea a los usuarios para que no inicien ninguna aplicación, excepto las que se permiten y no están prohibidas en las reglas de control de aplicaciones."	EXIGIDO	CUMPLE
2.59	El componente de control de aplicaciones debe crear una imagen propietaria de los programas que garantizan el funcionamiento normal del sistema operativo	EXIGIDO	CUMPLE
2.60	El componente de control de aplicaciones debe realizar un inventario de los archivos con los siguientes formatos: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX y SCR, cuando se añade contenido manualmente	EXIGIDO	CUMPLE
2.61	La solución debe incluir características básicas de Endpoint Detection and Response (EDR)	EXIGIDO	CUMPLE
2.62	La solución debe permitir agregar un Widget de alertas de EDR que muestre información sobre la cantidad de alertas en los dispositivos durante el último mes	EXIGIDO	CUMPLE
2.63	La solución debe contar con la capacidad de mostrar toda la información disponible sobre la amenaza detectada	EXIGIDO	CUMPLE
2.64	La solución debe proveer un gráfico de la cadena de desarrollo de amenazas que proporcione información visual sobre los objetos involucrados, como procesos clave en el dispositivo, conexiones de red, bibliotecas y subárboles de registro.	EXIGIDO	CUMPLE

Abog. Mariel Contrera C
Asesora Jurídica
INDERT

Fernández
Director
Sistemas Informáticos
INDERT

Peter Polka.

C.P Pablo A. Velázquez
Jefe Dpto. de Análisis y Evaluación
INDERT

Ítem N° 3 Renovación de Licencias – Protección de copias de seguridad– Barracuda Backup 490 con licenciamiento – 1 año

Nº	Especificaciones Técnicas	Mínimo Exigido	SEKIURA S.A.C.E.I. Cumple con las especificaciones requeridas (si/no)
3.1	La plataforma de backup y recuperación a desastres debe ser ofrecida solamente en arquitectura de Appliance de propósito único de Backup "Appliance PPBA", con almacenamento y software de backup en el mismo appliance. No serán aceptas soluciones de software de respaldos con almacenamiento storage apartados.	EXIGIDO	CUMPLE
3.2	La licencia de la plataforma de backup y recuperación a desastres debe gestionar 12TB de almacenamiento de datos integrada en el appliance	EXIGIDO	CUMPLE
3.3	La licencia de backup y recuperación a desastres debe permitir al administrador elegir entre administrar la plataforma localmente, o por medio de una consola de gestión centralizada desde la nube.	EXIGIDO	CUMPLE
3.4	La licencia de backup y recuperación a desastres debe permitir actuar en el escenario de replicación a otro appliance. Sea como appliance que envía datos a ser replicados a uno a múltiplos appliances, o un appliance que recibe datos desde uno o múltiples appliances	EXIGIDO	CUMPLE
3.5	La licencia de backup y recuperación a desastres debe permitir la utilización de agentes ilimitados, sin coste adicional a. Agentes para Windows Windows Server 2016 i. Windows Server 2012 ii. Windows Server 2008 iii. Windows Server 2003 SP2+ iv. Windows 8 v. Windows 7 vi. Windows Vista SP1+ vii. Windows XP SP3+ b. Agentes para Linux i. Kernel 2.6.16 32 Bits ii. Kernel 2.6.16 64 Bits	EXIGIDO	CUMPLE
3.6	La licencia de backup y recuperación a desastres debe ser compatible con las siguientes aplicaciones en cantidad ilimitada, sin coste adicional a. Microsoft Exchange i. Respaldo de la BBDD ii. Respaldo de mensajes iii. Respaldo de Carpetas Exchange individuales b. Microsoft SQL Server c. Microsoft Active Directory d. Microsoft SharePoint SQL Database e. Oracle f. IBM Domino g. GroupWise Message-Level h. Network Addressable Storage – NAS	EXIGIDO	CUMPLE
3.7	La plataforma de backup y recuperación a desastres debe cumplir con la funcionalidad "Bare Metal Recovery" por medio de midia de recuperación con soporte a 32 y 64 bits, permitiendo realizar el recovery tanto por el appliance, asi como en la nube.	EXIGIDO	CUMPLE
3.8	La licencia de backup y recuperación a desastres debe ser compatible con las siguientes hypervisores y proveer respaldo granular a sus máquinas virtuales en cantidad ilimitada, sin coste adicional a. Vmware i. sin necesidad de instalar agentes, debe poseer integración transparente via APIs que deben permitir integración transparente para respaldar todas sus máquinas virtuales) b. Microsoft Hyper-V i. Instalación de un único agente en el Microsoft HyperV Server debe permitir integración transparente para respaldar todas sus máquinas virtuales	EXIGIDO	CUMPLE
3.9	La licencia de backup y recuperación a desastres debe ser compatible con las siguientes hypervidores y proveer respaldo granular a sus máquinas virtuales en cantidad ilimitada, sin coste adicional • Nivel de host: VMware vSphere, Microsoft Hyper-V • Nivel de invitado: Citrix XenServer, Oracle VM, Red Hat Enterprise Virtualization y KVM	EXIGIDO	CUMPLE
3.10	La licencia de backup y recuperación a desastres debe tener la capacidad de realizar detección de cambios y debe realizar respaldos incrementales para realizar el respaldo de los datos que cambian con el tiempo	EXIGIDO	CUMPLE

C.P Pablo A. Velázquez
Jefe Dpto. de Análisis y Evaluación
ANDERT

Juan Fernández
Director
ANDERT

Asesora Jurídica

3.11	La plataforma de backup y recuperación a desastres debe tener la capacidad de realizar de duplicacion sin la necesidad de licenciamento de forma ilimitada para realizar de duplicacion en todos los orígenes de datos configurados en el appliance.	EXIGIDO	CUMPLE
3.12	La plataforma de backup debe ofrecer almacenamiento en la nube para la replicación fuera del sitio y recuperación ante desastres. Los datos almacenados en la nube deben ser reflejado entre las infraestructuras de almacenamiento mismo que estas estén físicamente separados en distintos datacenters.	EXIGIDO	CUMPLE
3.13	La plataforma de backup y recuperación a desastres debe ofrecer cifrado mínimo de 256 bits para encriptar los datos a ser almacenados. Además, los datos siempre deben ser transmitidos (entre equipos y hacia la nube) usando transporte en protocolo seguro y cifrado mínimo de 256 bits	EXIGIDO	CUMPLE
3.14	La plataforma de backup y recuperación a desastres debe ofrecer debe ofrecer la limitación de velocidad utilizando mecanismo inteligentes de "QoS" propios para los datos enviados fuera del sitio con la finalidad de minimizar el impacto de la replicación en la utilización de los enlaces de Internet disponibles.	EXIGIDO	CUMPLE
3.15	La plataforma de backup y recuperación a desastres debe ser capaz de restaurar archivos individuales directamente desde la nube hasta cualquier dispositivo conectado en la red o internet, hasta mismos dispositivos mobiles	EXIGIDO	CUMPLE
3.16	La plataforma de backup y recuperación a desastres debe permitir la realización de tareas automatizada de respaldos	EXIGIDO	CUMPLE
3.17	La plataforma de backup y recuperación a desastres debe proporcionar notificaciones automáticas de los éxitos y fallos de los respaldos, la disponibilidad del dispositivo, y alertas de errores críticos del sistema	EXIGIDO	CUMPLE
3.18	La plataforma de backup y recuperación a desastres debe ofrecer actualizaciones automáticas de software y el acceso a las nuevas funcionalidades de firmware durante el periodo de suscripción.	EXIGIDO	CUMPLE
3.19	La Empresa Oferente debe contar como mínimo con dos técnicos certificados de la marca	EXIGIDO	CUMPLE
3.20	La plataforma de backup y recuperación a desastres debe ofrecer opciones flexibles basados en el tiempo de retención y control de versiones que no restringen el número de revisiones o el período de tiempo en el que los datos se pueden mantener almacenados en el appliance.	EXIGIDO	CUMPLE

Abog. Mariel Contrera C
Asesora Jurídica
INDERT

Juan Fernández
Director
Dirección de Sistemas Informáticos
INDERT

Peter Poka.

C.P Pablo A. Velázquez
Jefe Dpto. de Análisis y Evaluación
INDERT

Ítem N° 4 Renovación de Licencias – Protección de Firewall perimetral – WatchGuard Firebox M370 con licenciamiento – 1 año

Nº	Especificaciones Técnicas	Mínimo Exigido	SEKIURA S.A.C.E.I. Cumple con las especificaciones requeridas (si/no)
4.1	Actualización de la versión del software a la última versión compatible definida por el administrador del contrato durante los primeros 6(seis) meses de contrato. Se expedirán certificados de capacitación.	EXIGIDO	CUMPLE
4.2	Actualización a la última versión de firmware disponible.	EXIGIDO	CUMPLE
4.3	Actualización de versiones por un período de 1 año	EXIGIDO	CUMPLE
4.4	Herramientas para incluir en la solución a) Intrusion Prevention Service (IPS) b) App Control c) WebBlocker d) spamBlocker e) Gateway Antivirus f) Reputation Enable Defense (RED) g) Network Discovery	EXIGIDO	CUMPLE
	CONCIDERACIONES ESPECIFICAS		
4.5	Actualización de versiones durante todo el periodo de licenciamiento	EXIGIDO	CUMPLE
4.6	Autorización del fabricante para proveer el software y brindar soporte	EXIGIDO	CUMPLE
4.7	Soporte permanente para todos los clientes, en todo momento, las 24 horas del día, los 7 días de la semana)	EXIGIDO	CUMPLE
4.8	Se deberá contar con toda la solución implementada en un plazo máximo de 30 días calendario desde la firma del contrato.	EXIGIDO	CUMPLE
4.9	Capacitación local del oferente para administración y configuración para 2 (dos) técnicos. La carga horaria debe ser de 10 horas y realizada en fecha	EXIGIDO	CUMPLE
4.10	El Oferente deberá contar con al menos 3 (tres) años de Experiencia implementando el UTM Watchguard y/o Software de Seguridad	EXIGIDO	CUMPLE
4.11	El oferente deberá contar con al menos 5 (cinco) Referencias de Clientes en donde se haya implementado soluciones de UTM Watchguard Firebox y/o Software de Seguridad en entes del Estado o Privados en los últimos 3 (tres) años (2021/2022/2023) en donde deberá presentar copia de Contratos o de Facturas y una carta de Referencia que avale la comercialización e implementación exitosa del Software ofertado dentro del Territorio Nacional.	EXIGIDO	CUMPLE

Abog. Mariel Contrera
Asesora Jurídica
INDERT

Juan Fernández
Director
Dirección de Sistemas Informáticos
INDERT

C.P Pablo A. Velázquez
Jefe Dpto. de Análisis y Evaluación
INDERT

ASPECTOS GENERALES	SEKIURA S.A.C.E.I. Cumple con las especificaciones requeridas (si/no)
El proveedor local deberá contar con por lo menos 1 técnico con certificación CEH o CEH MASTER o similar.	CUMPLE
El proveedor local deberá contar como mínimo con 3 técnicos certificados con las certificaciones avanzadas del producto de detección y respuesta EDR	CUMPLE
El proveedor local deberá contar como mínimo con 3 técnicos con certificaciones de cifrado.	CUMPLE
El proveedor local deberá contar con por lo menos 3 técnicos con certificaciones en protección de servidores de correo antispam.	CUMPLE
Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar certificados de inscripción en IPS.	CUMPLE
Contar con 10 contratos o facturas de la provisión de Software de Ciber seguridad entre los años 2021, 2022 y 2023.	CUMPLE
El proveedor local deberá contar con el mayor nivel de certificación/partnership posible la marca ofertada, para garantizar el buen servicio y respaldo del soporte local.	CUMPLE
l proveedor local deberá tener la Certificación ISO 9001: Sistema de Gestión de Calidad y la Certificación ISO 27001: Sistema de Gestión de Seguridad de la Información para garantizar el buen servicio y respaldo del soporte local.	CUMPLE
El proveedor deberá presentar autorización del fabricante expresamente dirigido a la convocante refiriendo el nro. de ID del llamado.	CUMPLE
El fabricante de las soluciones ofertadas debe brindar soporte a través de una página web, email y línea telefónica.	CUMPLE
El fabricante de las soluciones ofertadas debe contar con por lo menos 25 años de presencia en el mercado global.	CUMPLE
El fabricante de las soluciones ofertadas debe contar con un equipo de investigación global y con presencia de por lo menos cinco (5) analistas de investigación de amenazas en Latinoamérica, dedicados exclusivamente a la investigación y el análisis de amenazas para la región.	CUMPLE
El fabricante de las soluciones ofertadas debe contar con experiencia probada en el descubrimiento de vulnerabilidades desconocidas, APTs y malware avanzado y debe haber descubierto al menos dos (2) vulnerabilidades agregadas a la lista de Common Vulnerabilities and Exposures (CVE) en los últimos meses.	CUMPLE
DESPLIEGUE Y CAPACITACIÓN:	**SEKIURA S.A.C.E.I. Cumple con las especificaciones requeridas (si/no)**
El oferente adjudicado deberá contemplar el sistema operativo y la base de datos requeridos para la implementación de la solución, y deberá presentar la documentación y licencias correspondientes para el plazo contractual establecido.	CUMPLE
Se deberá incluir la instalación de la solución, el acompañamiento en el despliegue y posteriormente deberá realizar una capacitación acerca del uso y configuración de la solución a los funcionarios del departamento de TI.	CUMPLE
Se deberá incluir la asistencia y soporte técnico durante el periodo de validez de la licencia, para casos de mal funcionamiento de la solución.	CUMPLE

12. VERIFICACIÓN DE LA CAPACIDAD FINANCIERA

Se procede al análisis de la situación financiera conforme al Balance y Estado de Resultado de los años (2021, 2022, 2023) presentada por la firma CORPORATION SEKIURA S.A.C.E.I.

SITUACIÓN FINANCIERA DE LA FIRMA SEKIURA S.A.C.E.I.						
Descripción	**Cálculos**			**Índices**		
Indicadores	**2021**	**2022**	**2023**	**Promedio**	**Coefic**	**Parámetros de referencia**
Índice de liquidez	3.858.505.966	5.926.595.553	6.790.123.192	5.525.074.904		Mayor o igual que 1 en promedio en los 3 últimos años.-
Activo corriente					1,67	
Pasivo corriente	2.521.355.843	4.166.505.289	3.225.777.695	3.304.546.276		
Endeudamiento	2.521.355.843	4.166.505.289	3.225.777.695	3.304.546.276		No debe ser mayor que 0.80 en promedio en los 3 últimos años.-
Pasivo Total					0,35	
Activo Total	6.198.999.052	10.158.501.507	11.603.828.177	9.320.442.912		
Rentabilidad	834.522.065	2.314.252.009	2.386.152.264	1.844.975.446		No deberá ser negativo (-) promedio en los 3 últimos años.-
Utilidad del ejercicio					30,67	
Patrimonio Neto	3.677.843.209	5.991.895.218	8.378.048.482	6.015.928.970		

C.P. Fabiana A. Velázquez
Jefe Dpto. de Análisis y Evaluación
INDERT

J. M. Fernández
Director
Dirección de Sistemas Informáticos
INDERT

Abog. Mariel Contrera C.
Asesora Jurídica
INDERT

15

13. RECOMENDACIÓN DE ADJUDICACIÓN:

En atención a lo precedentemente enunciado, y al examen de la evidencia documental presentada por la firma **CORPORATION SEKIURA S.A.C.E.I.**, el presente Comité de Evaluación determina que las oferta analizada precedentemente se ajustan sustancialmente a los documentos de contratación y está calificada para ejecutar el contrato en forma satisfactoria; por lo cual el Comité de Evaluación recomienda la adjudicación para la presente **LICITACIÓN DE MENOR CUANTÍA NACIONAL N° 06/2024 "RENOVACION DE LICENCIAS ANTIVIRUS" ID N° 449.290,** a la firma **CORPORATION SEKIURA S.A.C.E.I. con RUC N° 80070889-0 por la suma de Gs. 333.150.000 (Guaraníes trescientos treinta y tres millones ciento cincuenta mil) IVA INCLUIDO,** ***Salvo mejor parecer de la Máxima Autoridad,*** conforme al siguiente detalle:

RENOVACION DE LICENCIAS ANTIVIRUS				
N° de ítem	Descripción	Cantidad	CORPORATION SEKIURA S.A.C.E.I.	
			Precio Unitario	Precio Total IVA Incluido
1	Renovación de Licencias Kaspersky Endpoint Security for Business con servicio de Instalación y Soporte por 1 año.-	475	464.000	220.400.000
2	Renovación de Licencias Kaspersky Security for Mail Server con servicio de Instalación y Soporte por 1 año.-	200	244.000	48.800.000
3	Renovación de Licencias – Protección de copias de Seguridad – Barracuda 490 con licenciaciamiento por 1 año.-	1	49.000.000	49.000.000
4	Renovación de Licencias – Protección de Firewall perimetral – WatchGuard Firebox M370 con licenciamiento por 1 año.	1	14.950.000	14.950.000
			TOTAL:	**333.150.000**

El método de adjudicación es *POR EL TOTAL.-*

14. CONCLUSIÓN:

La Recomendación de adjudicación se realiza considerando los aspectos indicados precedentemente, el cumplimiento de las ofertas respecto a las condiciones legales y técnicas, calificación y la capacidad necesaria para proveer los bienes.-

Todas las documentaciones mencionadas en el presente informe, como así también las recomendaciones de adjudicación forman parte del presente documento.-

No habiendo otro tema que tratar se procede a la lectura y ratificación del contenido del presente informe de evaluación, procediéndose a la firma correspondiente por parte de los funcionarios arriba citados en prueba de conformidad en 2 (dos) copias de un mismo tenor y a un solo efecto.-

Sr. Peter Poka
Comité de Evaluación

Juan Fernández
Comité de Evaluación

Abg. Mariel Contrera
Comité de Evaluación

C.P. Pablo Velazquez
Comité de Evaluación