INFORME DE EVALUACIÓN N.° 10/2024

LLAMADO ANTSV N° 04/2024 LICITACIÓN MENOR CUANTÍA NACIONAL - SERVICIO DE SUSCRIPCIÓN DE SOFTWARE ANTIVIRUS DE LA ANTSV - ID NRO. 444175

En la ciudad de Asunción, Capital de la República del Paraguay, siendo las 13:00 horas del día 03 de octubre de 2024, en la sala de reuniones de la Agencia Nacional de Tránsito y Seguridad Vial (ANTSV), sito en las calles Guido Spano Nro. 595 esq. 23 de Octubre, se reúnen la **ABG. NATHALIA DE LA VEGA PÉREZ**, Profesional Administrativa de la Secretaría General, el **LIC. JUN DANIEL VALLEJOS TANIWAKI.**, Jefe de Unidad Técnica de Proyectos de la DNLCAT y el **SR. ALEJANDRO RAMÓN SOLÍS ZENA**, Jefe de Patrimonio; para realizar la evaluación de las ofertas presentadas en el Proceso Licitatorio ANTSV N° 04/2024 Licitación de Menor Cuantía Nacional "*SERVICIO DE SUSCRIPCIÓN DE SOFTWARE ANTIVIRUS DE LA ANTSV*" - ID N° 444175

Los funcionarios se encuentran autorizados según Resolución ANTSV N.° 013/2024 **POR LA CUAL SE CONFORMA EL COMITÉ DE EVALUACIÓN DE OFERTAS, PARA EL ANÁLISIS TÉCNICO, JURÍDICO, Y ECONÓMICO-FINANCIERO**, para realizar las evaluaciones y recomendar la adjudicación del llamado.

1) APERTURAS DE OFERTAS:

De acuerdo al procedimiento previsto en el Decreto Reglamentario N.° 2264/24 y concordantes, el proceso de Apertura de Ofertas ha sido llevado a cabo el día 27 de septiembre del 2024.

El Acta de Apertura física de Sobres se ha realizado en la misma fecha a las 10:15 hs. hasta las 10:40 hs., en virtud a lo establecido en el SICP, se procedió a la apertura de sobres, dejándose expresa constancia de las siguientes ofertas abiertas en el acto:

N°	Oferentes presentados	RUC	Precio de la Oferta (IVA incluido)
1	SEGEL S.A.	80026570-0	Gs. 36.548.120
2	ARIVOIR S.A.	80049511-0	Gs. 43.400.000
3	INFORMATION TECHNOLOGY CONSULTING SUPPORT SOCIEDAD ANÓNIMA	80046953-4	Gs. 42.820.190

El proceso de apertura de ofertas por parte de esta convocante se llevó a cabo con la presencia del LIC. **PABLO SANCHEZ** – Jefe del Dpto. de Adquisiciones DOC - ANTSV, y la C.P. **NATHALIA DOMECQ** – Jefa del Dpto. de Programación y Evaluación de la DOC por la convocante.

Abg. Nathalia de la Vega Pérez
Profesional Administrativa
Secretaría General
ANTSV

Alejandro R. Solís Zena
Jefe Dpto. de Patrimonio
ANTSV

Lic. Jun Daniel Vallejos Taniwaki
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

2) OBSERVACIONES REALIZADAS EN LA APERTURA:

Observación a la oferta: 80049511-0 – ARIVOIR S.A

Observación a la oferta	Observador	Representante	Fecha/Hora
No presenta la certificación de la Garantía de Mantenimiento de Oferta y No presenta constancia SIPE.	80026570-0 – SEGEL S.A	María Cristina Balbuena	2024-09-27 10:37:40

Observación a la oferta: 80046953-4 – INFORMATION TECHNOLOGY CONSULTING SUPPORT S.A

Observación a la oferta	Observador	Representante	Fecha/Hora
El certificado de cumplimiento tributario se encuentra vencido	80026570-0 – SEGEL S.A	María Cristina Balbuena	2024-09-27 10:37:40

3) TABLA COMPARATIVA DE PRECIOS DE LAS OFERTAS AJUSTADA POR ERRORES ARITMÉTICOS Y ANÁLISIS DE PRECIOS OFERTADOS:

TABLA COMPARATIVA DE PRECIOS DE LAS OFERTAS AJUSTADA POR ERRORES ARITMÉTICOS Y ANÁLISIS DE PRECIOS OFERTADOS

Ítems del llamado "SUSCRIPCIÓN DE SOFTWARE ANTIVIRUS DE LA ANTSV" - ID NRO. 444.175

INFORMATION TECHNOLOGY CONSULTING SUPPORT SOCIEDAD ANONIMA

Ítem	Descripción del Bien	Unidad de Medida	Presentación	Cantidad	Precio Unitario (IVA incluido) Gs.	Precio Referencial de la Convocante	Análisis del Precio s/ PBC	Precio total ofertado
1	SOFTWARE ANTIVIRUS PARA COMPUTADORA	UNIDAD	EVENTO	70	611.717	611.717	0,00	42.820.190

TABLA COMPARATIVA DE PRECIOS DE LAS OFERTAS AJUSTADA POR ERRORES ARITMÉTICOS Y ANÁLISIS DE PRECIOS OFERTADOS

Ítems del llamado "SUSCRIPCIÓN DE SOFTWARE ANTIVIRUS DE LA ANTSV" - ID NRO. 444.175

SEGEL S.A.

Ítem	Descripción del Bien	Unidad de Medida	Presentación	Cantidad	Precio Unitario (IVA incluido) Gs.	Precio Referencial de la Convocante	Análisis del Precio s/ PBC	Precio total ofertado
1	SOFTWARE ANTIVIRUS PARA COMPUTADORA	UNIDAD	EVENTO	70	522.116	611.717	-14,65	36.548.120

Abg. Natalia de la Vega Pérez
Profesional Administrativa
Secretaría General
ANTSV

Alejandro J. Solís Zena
Jefe Dpto. de Patrimonio
ANTSV

Lic. Jun Daniel Vallejos Taniwaki
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

TABLA COMPARATIVA DE PRECIOS DE LAS OFERTAS AJUSTADA POR ERRORES ARITMÉTICOS Y ANÁLISIS DE PRECIOS OFERTADOS

Ítems del llamado "SUSCRIPCIÓN DE SOFTWARE ANTIVIRUS DE LA ANTSV" - ID NRO. 444.175

ARIVOIR S.A.

Ítem	Descripción del Bien	Unidad de Medida	Presentación	Cantidad	Precio Unitario (IVA Incluido) Gs.	Precio Referencial de la Convocante	Análisis del Precio s/ PBC	Precio total ofertado
1	SOFTWARE ANTIVIRUS PARA COMPUTADORA	UNIDAD	EVENTO	70	620.000	611.717	1,35	43.400.000

OFERTA PRESENTADA POR LA EMPRESA ITCS S. A

NRO_ GRUPO	CÓDIGO_ CATÁLOGO	DESCRIPCIÓN	ATRIBUTOS	CANTIDAD	Precio Unitario (IVA Incluido)	CARACTERÍSTICAS
1	43233205-001	Software antivirus para computadora.	Unidad de medida: Unidad. Presentación: Unidad	70	611.717	Marca: SOPHOS. Fabricante: SOPHOS. Procedencia: EE.UU.
					Precio Total	**42.820.190**

OFERTA PRESENTADA POR LA EMPRESA SEGEL S. A

NRO_ GRUPO	CÓDIGO_ CATÁLOGO	DESCRIPCIÓN	ATRIBUTOS	CANTIDAD	Precio Unitario (IVA Incluido)	CARACTERÍSTICAS
1	43233205-001	Software antivirus para computadora.	Unidad de medida: Unidad. Presentación: Unidad	70	522.116	Marca: Kaspersky. Fabricante: Kaspersky. Procedencia: Rusia.
					Precio Total	**36.548.120**

OFERTA PRESENTADA POR LA EMPRESA ARIVOIR S. A

NRO_ GRUPO	CÓDIGO_ CATÁLOGO	DESCRIPCIÓN	ATRIBUTOS	CANTIDAD	Precio Unitario (IVA Incluido)	CARACTERÍSTICAS
1	43233205-001	Software antivirus para computadora.	Unidad de medida: Unidad. Presentación: Unidad	70	620.000	Marca: ESET. Fabricante: ESET. Procedencia: ESLOVAQUIA.
					Precio Total	**43.400.000**

Abg. Nathalia de la Vega Pérez
Profesional Administrativa
Secretaría General
ANTSV

Lic. Jun Daniel Vallejos Tauiwaki
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

4) **ANÁLISIS DE LAS DOCUMENTACIONES PRESENTADAS.**

Documentos Sustanciales:

4.1 ESTUDIO DE LAS OFERTAS: El estudio fue realizado conforme a lo establecido en el Pliego de Bases y Condiciones, para lo cual se han adoptado los siguientes pasos:

a) Verificación de Documentos:

1. **Documentos sustanciales**: Verificación del cumplimiento de cada oferta respecto al suministro de la documentación básica de carácter sustancial solicitado. En este punto serán eliminadas aquellas ofertas que no cumplan con la documentación solicitada o sea insatisfactoria por presentar desviaciones u omisiones sustanciales, las cuales se indican a continuación:

   - Garantía de Mantenimiento de Oferta debidamente extendida;
   - Formulario de Oferta debidamente firmado y completado;

   En el caso que suscriba la oferta otra persona en su representación, deberá acompañar una fotocopia simple de su cédula de identidad y una fotocopia autenticada del poder suficiente otorgado por Escritura Pública para presentar la oferta y representarlo en los actos de la licitación. No es necesario que el Poder esté inscripto en el Registro de Poderes.

	CUMPLE/NO CUMPLE	CUMPLE/NO CUMPLE	CUMPLE/ NO CUMPLE
SEGEL S.A	CUMPLE (fs. 0000001/3)	CUMPLE (fs. 000004)	CUMPLE a) (fs. 000012/18) b) (fs. 00008) c) (fs. 00008) d) (fs. 00008)
ARIVOIR S. A	CUMPLE (fs. 0000002/4)	CUMPLE (fs. 0000005/6)	NO CUMPLE a) NO CUMPLE. b) NO CUMPLE. c) (fs. 000009) d) NO CUMPLE.
ITCS S. A	CUMPLE (fs. 0000005/7)	CUMPLE (fs. 0000008/9)	CUMPLE a) b), c): fs. 000002 según SIPE N° 1812969. / d) (fs. 00010)

CONCLUSIÓN:

En cuanto a este punto, se aclara que las ofertas presentadas por SEGEL y ITCS, cumplen con las documentaciones sustanciales para continuar con el análisis de las demás documentaciones en conformidad al Pliego de Bases y Condiciones.

Sin embargo la empresa ARIVOIR S.A, no cumple con la documentación sustancial, quedando descalificada en esta instancia de evaluación, como se detalla en el cuadro precedente.

5) **REQUISITOS DE CALIFICACIÓN Y CRITERIOS DE EVALUACIÓN.**

Para el análisis de las documentaciones formales de la firma **SEGEL S.A.** y la firma **ITCS S.A.** se cotejan los siguientes puntos establecidos en el Pliego de Bases y Condiciones:

1.1. **Requisitos de Calificación Legal:** Los oferentes deberán declarar que no se encuentran comprendidos en las limitaciones o prohibiciones para contratar con el Estado, contempladas en

Abg. Nathalia de la Vega Pérez
Profesional Administrativa
Secretaría General
ANTSV

Alejandro A. Solís Zena
Jefe Dpto. de Patrimonio
ANTSV

Lic. Juri Daniel Vallejos Tanimaki
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

el artículo 21 de la Ley N° 7021/23, en concordancia con el Artículo 19 de su Decreto Reglamentario. Esta declaración forma parte del formulario de oferta en los casos que el procedimiento de contratación sea convencional y el formulario de oferta electrónica en el caso que se utilice el modelo de oferta electrónica.

Serán desechadas las ofertas de los oferentes que se encuentren comprendidos en las prohibiciones o limitaciones para presentar propuestas y contratar con el estado, a la hora y fecha límite de presentación de ofertas o a la fecha de firma del contrato.

Calificación legal		
Documentos.	**SEGEL S.A**	**ITCS S. A**
1. Formulario de ofertas que incluye la declaratoria debidamente firmada.	PRESENTA	PRESENTA
2. Verificación si los oferentes o sus representantes, se hallan comprendidos en el presupuesto del inciso a) y b) del artículo 21 de la Ley N.° 7021/2022.	MARLENE PEREIRA PEREIRA, con CI N° 3.197.459, no registra datos, se verifica desde la página web	CESAR ROMEO ACOSTA FORMOSO, con CI N° 3.298.115, no registra datos, se verifica desde la página web.
3.Verificación si los oferentes han proporcionado el formulario de Declaración de Miembros y verificación sobre si poseen *"Sanciones a Proveedores"*.	PRESENTA FORMULARIO.	PRESENTA FORMULARIO.
	Según se verifica en EL PORTAL DE LA DNCP: EL OFERENTE NO REGISTRA SANCIONES VIGENTES. (fs. 0000010/11)	Según se verifica en EL PORTAL DE LA DNCP: EL OFERENTE NO REGISTRA SANCIONES VIGENTES. (fs. 00000011/12)

CONCLUSIÓN:

Se constata respecto a los representantes legales, socios y/o accionistas de las firmas ***SEGEL S.A*** *y* ***INFORMATION TECHNOLOGY CONSULTING SUPPORT SOCIEDAD ANÓNIMA****., que ninguno de los representantes legales, se encuentran entre las prohibiciones establecidas en el Pliego de Bases y Condiciones con relación a este punto de la evaluación.*

6) <u>REQUISITOS DOCUMENTALES PARA EVALUACIÓN DE LAS CONDICIONES DE PARTICIPACIÓN.</u>

Documentos formales: Seguidamente se procede a verificar que los oferentes hayan proveído los formularios de carácter formal y la documentación que avale la calificación y competencia requerida para la evaluación de este punto.

Abg. Natalia de la Vega Pérez
Profesional Administrativa
Secretaría General
ANTSV

Alejandro Ramón Solís Zena
Jefe Dpto. de Patrimonio
ANTSV

Lic. Jun Daniel Vallejos Tanlwaki
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

REQUISITOS DOCUMENTALES PARA LA EVALUACIÓN DE LAS CONDICIONES DE PARTICIPACIÓN	CUMPLE/NO CUMPLE	CUMPLE/NO CUMPLE
	SEGEL S.A	ITCS S.A.
1. Formulario de Oferta (*)	**CUMPLE** (fs. 0000001/3)	**CUMPLE** (fs. 0000005/7)
2. Garantía de Mantenimiento de Oferta (*)	**CUMPLE** (fs. 000004)	**CUMPLE** (fs. 0000008/9)
3. Certificado de Cumplimiento con la Seguridad Social. (**)	**CUMPLE** (fs. 0000006)	**CUMPLE** (fs. 0000003)
4. Certificado de Producto y Empleo Nacional, emitido por el MIC, en caso de contar. (**)	**NO PRESENTA**	**NO PRESENTA**
5. Certificado de Cumplimiento Tributario. (**)	**CUMPLE** (fs. 0000007)	**CUMPLE** (fs. 0000003)
6. Patente Comercial del municipio en donde esté asentado el establecimiento principal del oferente. (**)	**CUMPLE** SEGÚN RESPUESTA A NOTA ANTSV CEO N° 01/2024	**CUMPLE** SEGÚN SICP (fs. 0000002)
7. Declaración Jurada de "Declaración de Personas", de conformidad con el formulario estándar - Sección Formularios (**)	**CUMPLE** (fs. 0000010/11)	**CUMPLE** (fs. 00000008/9)
[redacted]		
8.1 Oferentes Individuales. Personas Físicas.		
a. Fotocopia simple de la Cédula de Identidad del firmante de la oferta. (*)	**NO APLICA**	**NO APLICA**
b. Constancia de inscripción en el Registro Único de Contribuyentes – RUC (*)	**NO APLICA**	**NO APLICA**
c. En el caso que suscriba la oferta otra persona en su representación, deberá acompañar una fotocopia simple de su cédula de identidad y una fotocopia simple del poder suficiente otorgado por Escritura Pública para presentar la oferta y	**NO APLICA**	**NO APLICA**

Abg. Nathalia de la Vega Pérez
Profesional Administrativa
Secretaría General
ANTSV

Alejandro R. Solís Zena
Jefe Dpto. de Patrimonio
ANTSV

Lic. Juan Daniel Vallejos Taniwaki
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

representarlo en los actos de la licitación. No es necesario que el poder esté inscripto en el Registro de Poderes. (*)		
8.2. Personas Jurídicas.		
1. 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 inscritos en la Sección Personas Jurídicas de la Dirección de Registros Públicos. (*)	**CUMPLE** SEGÚN (fs. 0000029/33)	**CUMPLE** SEGÚN SICP (fs. 0000013)
2. Constancia de inscripción en el Registro Único de Contribuyentes. (*)	**CUMPLE** SEGÚN (fs. 0000016/17)	**CUMPLE** SEGÚN SICP (fs. 0000013)
3. Fotocopia simple de los documentos de identidad de los representantes o apoderados de la sociedad. (*)	**CUMPLE** SEGÚN (fs. 0000018/19)	**CUMPLE** SEGÚN (fs. 0000033)
d- 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** SEGÚN (fs. 000020/23)	**CUMPLE** según Nota del 16/09/2024 en respuesta a lo solicitado en la nota ANTSV/CEO N°2
8.3. Oferentes en Consorcio.	**NO APLICA**	**NO APLICA**

CONCLUSIÓN: *Este Comité concluye que se verifican los* **REQUISITOS DOCUMENTALES PARA LA EVALUACIÓN DE LAS CONDICIONES DE PARTICIPACIÓN** *de los oferentes, con el análisis realizado a los documentos presentados por las firmas* SEGEL S.A. y INFORMATION TECHNOLOGY Y CONSULTING SUPPORT S.A. *los mismos cumplen con los requisitos documentales para evaluar el presente criterio, de conformidad al Pliego de Bases y Condiciones.*
Observaciones: Ninguna de las dos empresas ha presentado el Certificado de Producto y Empleo Nacional, emitido por el MIC. (**)

7) REQUISITOS DOCUMENTALES PARA LA EVALUACIÓN DE LA CAPACIDAD FINANCIERA.

Este Comité de Evaluación procedió seguidamente a verificar la capacidad financiera del Oferente presentados de conformidad a lo establecido en el Pliego de Bases y Condiciones del Llamado, según el siguiente detalle:

Para evaluar el presente criterio, el oferente deberá presentar las siguientes documentaciones:

Abg. Nathalia de la Vega Pérez
Profesional Administrativa
Secretaría General
ANTSV

Alejandro R. Solís Zena
Jefe Dpto. de Patrimonio
ANTSV

Lic. Juh Daniel Vallejos Taniwaki
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

CRITERIOS DE EVALUACIÓN DE LA CAPACIDAD FINANCIERA	SEGEL S.A.	ITCS S.A.
a. Ratio de Liquidez: activo corriente / pasivo corriente. Deberá ser igual o mayor que 1, en promedio, en los últimos años [2020,2022,2023)	CUMPLE – SEGÚN RTA. NOTA ANTSV/CEO N°1	CUMPLE – SEGÚN RTA. NOTA ANTSV/CEO N°2
b. Endeudamiento: pasivo total / activo total. No deberá ser mayor a 0,80 en promedio, en los últimos años [2020,2022,2023]	CUMPLE – SEGÚN RTA. NOTA ANTSV/CEO N°1	CUMPLE – SEGÚN RTA. NOTA ANTSV/CEO N°2
c. Rentabilidad: Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital. El promedio en los años [2020,2022,2023], no deberá ser negativo.	CUMPLE – SEGÚN RTA. NOTA ANTSV/CEO N°1	CUMPLE – SEGÚN RTA. NOTA ANTSV/CEO N°2

LLAMADO ANTSV N° 04/2024 LICITACIÓN MENOR CUANTÍA NACIONAL "SERVICIO DE SUSCRIPCION DE SOFTWARE ANTIVIRUS" ANTSV - ID N° 444175

Capacidad Financiera - Empresa: SEGEL S.A

Ratio de Liquidez	2020	2021	2022	Promedio Total	Coeficiente medio	Conclusión
Activo Corriente	28.187.565.559	34.929.968.269	40.700.745.991	34.606.093.273	2,01	Cumple
Pasivo Corriente	11.431.152.121	15.725.335.669	30.177.415.967	19.111.301.252		
Resultado	**2,47**	**2,22**	**1,35**	**2,01**		
Endeudamiento	**2020**	**2021**	**2022**	**Promedio Total**	**Coeficiente medio**	**Conclusión**
Pasivo Total	15.563.974.390	1.986.157.938	30.177.415.967	15.909.182.765	0,36	Cumple
Activo Total	34.063.257.422	40.557.894.768	52.405.065.551	42.342.072.580		
Resultado	**0,46**	**0,05**	**0,58**	**0,36**		
Rentabilidad	**2020**	**2021**	**2022**	**Promedio Total**	**Coeficiente medio**	**Conclusión**
Utilidad del Ejercicio	2.325.870.363	2.197.453.798	1.530.912.754	2.018.078.972	0,12	Cumple
Capital	15.009.553.520	17.100.168.053	19.187.749.161	17.099.156.911		
Resultado	**0,15**	**0,13**	**0,08**	**0,12**		

Abg. Nathalia de la Vega Perez
Profesional Administrativa
Secretaría General
ANTSV

Alejandro R. Solís Zena
Jefe Dpto. de Patrimonio
ANTSV

Lic. Jun Daniel Vallejos Tanimaki
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

LLAMADO ANTSV N° 04/2024 LICITACIÓN MENOR CUANTÍA NACIONAL "SERVICIO DE SUSCRIPCIÓN DE SOFTWARE ANTIVIRUS" ANTSV - ID N° 444175						
Capacidad Financiera - Empresa: INFORMATION TECHNOLOGY Y CONSULTING SUPPORT S.A.						
Ratio de Liquidez	**2020**	**2021**	**2022**	**Promedio Total**	**Coeficiente medio**	**Conclusión**
Activo Corriente	6.717.153.071	13.538.293.067	18.000.594.730	12.752.013.623	**4,71**	**Cumple**
Pasivo Corriente	1.065.147.912	2.200.389.203	10.741.172.109	4.668.903.075		
Resultado	**6,31**	**6,15**	**1,68**	**4,71**		
Endeudamiento	**2020**	**2021**	**2022**	**Promedio Total**	**Coeficiente medio**	**Conclusión**
Pasivo Total	4.587.605.060	8.235.186.525	11.280.022.391	8.034.271.325	**0,60**	**Cumple**
Activo Total	7.307.452.770	14.545.209.881	19.041.658.999	13.631.440.550		
Resultado	**0,63**	**0,57**	**0,59**	**0,60**		
Rentabilidad	**2020**	**2021**	**2022**	**Promedio Total**	**Coeficiente medio**	**Conclusión**
Utilidad del Ejercicio	1.535.001.084	3.410.666.864	4.269.859.399	3.071.842.449	**1,54**	**Cumple**
Capital	1.000.000.000	2.500.000.000	2.500.000.000	2.000.000.000		
Resultado	**1,54**	**1,36**	**1,71**	**1,54**		

CONCLUSIÓN:

Este Comité concluye que se verifican las CAPACIDADES FINANCIERAS de los oferentes, con el análisis realizado a los documentos presentados por las firmas SEGEL S.A. y INFORMATION TECHNOLOGY Y CONSULTING SUPPORT S.A. *los mismos cumplen con los requisitos documentales para evaluar el presente criterio, de conformidad al Pliego de Bases y Condiciones.*

8) Requisitos documentales para la evaluación de la experiencia

a. **Experiencia requerida:** Este Comité de Evaluación procedió seguidamente a verificar la experiencia requerida a los Oferentes presentados de conformidad a lo establecido en el Pliego de Bases y Condiciones del Llamado, según el siguiente detalle:

CRITERIOS PARA LA EVALUACIÓN DE LA EXPERIENCIA REQUERIDA	SEGEL S.A.	ITCS S.A.
1. Demostrar la experiencia en provisión de licencias con facturaciones de venta, contratos y o recepciones finales u otros documentos, por un monto equivalente al 30 % como mínimo del monto total ofertado en el presente procedimiento de contratación, de los: últimos 4 años [2020, 2021, 2022, 2023]. Las sumatorias de las facturaciones deben alcanzar el porcentaje indicado, no será necesaria la presentación del porcentaje del monto establecido por cada año.	CUMPLE SEGÚN RTA. NOTA ANTSV/CEO N°1	CUMPLE SEGÚN RTA. NOTA ANTSV/CEO N°2

Abg. Natalia de la Vega Pérez
Profesional Administrativa
Secretaría General
ANTSV

Alejandro R. Solís Zena
Jefe Dpto. de Patrimonio
ANTSV

Lic. Jun Daniel Vallejos Tanimaki
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

CONCLUSIÓN:

Con respecto a este punto, este Comité Concluye que se verifican la **EXPERIENCIA REQUERIDA** de los oferentes, con el análisis realizado a los documentos presentados por la firma SEGEL S.A. y la firma ITCS S.A. constatándose que cumplen con los requisitos documentales para evaluar el presente criterio en conformidad al Pliego de Bases y Condiciones.

9) Requisitos documentales para evaluar el criterio de capacidad técnica

Este Comité de Evaluación procedió seguidamente a verificar la Capacidad Técnica requerida del Oferente presentado de conformidad a lo establecido en el Pliego de Bases y Condiciones del Llamado.

Capacidad Técnica	**Empresa SEGEL S.A.**	**Empresa ITCS**
El oferente deberá proporcionar evidencia documentada que demuestre su cumplimiento con los siguientes requisitos de capacidad técnica:		
1. Certificación ISO 9001/2015 o similar, la similitud debe basarse en los mismos criterios que solicita o certifica la norma ISO 9001/2015 con respecto a la calidad de la gestión de procedimientos de Provisión e integración de bienes y/o servicios.	Cumple	Cumple
2. El oferente deberá contar con al menos 2 técnicos con certificaciones de la marca ofertada.	Cumple	Cumple
3. El oferente deberá acreditarse como representante oficial o distribuidor autorizado del software y sus respectivas licencias, según se detalla:	Cumple	Cumple

El oferente deberá acreditarse como representante oficial o distribuidor autorizado por el fabricante del software ofertado manifestando que posee la capacidad para proveer la cantidad ofertada en el tiempo solicitado. En la misma, deberá constar que se encuentra en condiciones para proveer, instalar, configurar y soportar el software, según lo solicitado en la planilla de especificaciones técnicas, en caso de resultar adjudicatario.

Requisitos documentales para evaluar el criterio de capacidad técnica	**Empresa SEGEL S.A.**	**Empresa ITCS**
Los siguientes documentos serán los considerados para la evaluación del presente criterio:		
1. Certificación ISO 9001/2015 o similar	Presentado	Presentado
3. El oferente deberá contar con al menos 2 técnicos con certificaciones de la marca ofertada.	Presentado	Presentado
4 . El oferente deberá acreditarse como representante oficial o distribuidor autorizado por el fabricante del software ofertado manifestando que posee la capacidad para proveer la cantidad ofertada en el tiempo solicitado.	Presentado	Presentado

CONCLUSIÓN:

*Con respecto a este punto, este Comité Concluye que se verifica la **CAPACIDAD TÉCNICA** de los oferentes, con el análisis realizado a los documentos presentados por la firma **Empresa SEGEL S.A.** y la **Empresa ITCS S.A.** constatándose que cumplen con los requisitos documentales para evaluar el presente criterio en conformidad al Pliego de Bases y Condiciones.*

Abg. Nathalia de la Vega Pérez
Profesional Administrativa
Secretaria General
ANTSV

Alejandro R. Solís Zena
Jefe Dpto. de Patrimonio
ANTSV

Lic. Jun Daniel Vallejos Taniwaki
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

Especificaciones Técnicas.

Detalle de los bienes y/o servicios

Los bienes y/o servicios deberán cumplir con las siguientes especificaciones técnicas y normas:

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
Marca	Especificar	Exigido	Kaspersky	-	SOPHOS	-
Modelo	Especificar	Exigido	Kaspersky Next EDR Optimum	https://latam.kaspersky.com/next-edr-optimum?srsltid=AfmBOooqr7cOGTnFIF3VWkoMageVb7TjhRx_Pj4b85qNxW3QEtSnj8G	Central Intercept X Advanced	https://www.enterprisecav.com/Intercept-X-Adv.asp
Procedencia	Especificar	Exigido	Rusia	Según la página web oficial de la empresa su origen es Rusia. https://latam.kaspersky.com/about	EE.UU.	Según la página web oficial de la empresa su origen es Reino Unido. https://www.sophos.com/es-es/legal
Cantidad	70 (setenta) unidades	Exigido	70 unidades	-	70 unidades	-
Consola de Administración	La administración deberá ser a través de una consola central única, basada en web y en nube, que deberá contener todas las componentes para el monitoreo y control de la protección de los dispositivos	Exigido	Cumple	La administración se realiza a través de una consola web central, con opción de instalación en la nube	Cumple	Es una plataforma basada en la nube que centraliza la gestión de la protección de dispositivos, permitiendo el control desde cualquier lugar con acceso web.
	La consola deberá presentar un Dashboard con el resumen del estado de protección de los ordenadores y usuarios, así como indicar las alertas de eventos de criticidades alta, media e informativa	Exigido	Cumple	Proporciona un panel visual con alertas clasificadas por criticidad	Cumple	La consola incluye un tablero de control que muestra un resumen de los dispositivos protegidos y alertas críticas.
	Debe poseer un mecanismo de comunicación vía API, para su integración con otras soluciones de seguridad, como por ejemplo SIEM	Exigido	Cumple	Soporta integración con otros sistemas de seguridad mediante API	Cumple	Ofrece APIs que permiten la integración con sistemas de seguridad como SIEMs.
	La consola debe permitir la división de los ordenadores dentro de la estructura de administración en grupos	Exigido	Cumple	Permite la administración de dispositivos por grupos	Cumple	La consola permite organizar dispositivos en grupos personalizados para administrar configuraciones y políticas.
	Debe permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección.	Exigido	Cumple	Compatible con AD para la gestión de usuarios y grupos	Cumple	Integra con Active Directory para la gestión de usuarios y dispositivos.

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Debe poseer la posibilidad de aplicar reglas diferenciadas por grupos de usuarios, usuarios individuales, grupos de máquinas y equipos individuales	Exigido	Cumple	Soporta reglas para usuarios individuales y grupos	Cumple	Facilita la aplicación de políticas diferenciadas por grupos de usuarios o dispositivos.
	La instalación debe poder realizarse a través del cliente descargado de la consola central y también vía correo electrónico de configuración. El instalador debe permitir la distribución del cliente a través de Active Directory (AD) para múltiples máquinas.	Exigido	Cumple	Soporta instalación desde la consola central, vía correo electrónico o Active Directory	Cumple	Permite la instalación remota desde la consola y despliegue masivo a través de Active Directory.
	Proporcionar actualizaciones del producto y de las definiciones de virus y protección contra intrusos	Exigido	Cumple	Proporciona actualizaciones automáticas del producto y definiciones de virus	Cumple	Actualiza automáticamente tanto las definiciones de virus como el software.
	Debe permitir exclusiones de escaneo para un determinado sitio web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política.	Exigido	Cumple	Permite exclusiones a nivel de sitio web, archivo, carpeta o proceso	Cumple	La consola permite definir exclusiones a nivel global o para políticas específicas (webs, archivos, aplicaciones).
	La consola de administración debe permitir la definición de grupos de usuarios con diferentes niveles de acceso a la configuración, las políticas y los registros	Exigido	Cumple	Soporta niveles de acceso diferenciados	Cumple	Permite configurar permisos diferenciados para administradores con distintos roles.
	Actualización incremental, remota y en tiempo real, de las vacunas de los Antivirus y del mecanismo de verificación (Engine) de los clientes	Exigido	Cumple	Realiza actualizaciones incrementales en tiempo real	Cumple	Las actualizaciones se realizan de manera incremental y en tiempo real, sin interrumpir a los usuarios.
	Permitir la programación de la exploración contra virus con la posibilidad de seleccionar una máquina o grupo de máquinas, con periodicidad definida por el administrador	Exigido	Cumple	Soporta programación de escaneos periódicos de virus	Cumple	Facilita la programación de exploraciones personalizadas para dispositivos o grupos.
	Utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los clientes administrados.	Exigido	Cumple	Utiliza protocolos seguros estándar	Cumple	Toda la comunicación entre la consola y los dispositivos se realiza de forma segura mediante HTTPS.
	Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.	Exigido	Cumple	Soporta la configuración de mensajes en varios idiomas, incluido el español	Cumple	Los mensajes generados por el sistema están disponibles en español, o se pueden editar según sea necesario.

Abg. Nathalia de la Vega Pérez
Profesional Administrativa
Secretaria General
ANTSV

Alejandro R. Solís Zena
Jefe Dpto. de Patrimonio
ANTSV

Lic. Juan Daniel Vallejos Tanhwaki
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Permitir la exportación de los informes gerenciales a los formatos CSV y PDF	Exigido	Cumple	Proporciona informes exportables en ambos formatos	Cumple	Los informes pueden exportarse en formatos CSV y PDF.
	Los recursos del informe y el monitoreo deben ser nativos de la propia consola central de administración	Exigido	Cumple	Los informes son generados directamente desde la consola	Cumple	Los informes y opciones de monitoreo están integrados en la propia consola, sin necesidad de herramientas adicionales.
	Posibilidad de mostrar información como nombre de la máquina, versión del antivirus, sistema operativo, dirección IP, versión del motor, fecha de la actualización, fecha de la última verificación, eventos recientes y estado	Exigido	Cumple	Muestra información detallada de cada dispositivo administrado	Cumple	La consola muestra información completa sobre cada dispositivo, incluyendo IP, sistema operativo, y más.
	La comunicación debe permitir QoS para controlar el ancho de banda de red.	Exigido	Cumple	Soporta control de ancho de banda	Cumple	Permite gestionar el uso del ancho de banda para actualizaciones, ajustando según las necesidades de la red.
	Debe permitir seleccionar un grupo de equipos para aplicar la actualización para controlar el ancho de banda de red. La actualización de la versión debe ser transparente para los usuarios finales.	Exigido	Cumple	Permite la actualización por grupos sin afectar a los usuarios finales	Cumple	Se pueden seleccionar grupos de dispositivos para aplicar actualizaciones, minimizando el impacto en la red.
	La herramienta de administración centralizada debe administrar todos los componentes de la protección para estaciones de y debe diseñarse para administrar, supervisar y elaborar informes de endpoint.	Exigido	Cumple	La consola administra todos los aspectos de la protección en estaciones de trabajo	Cumple	Administra todas las funciones de seguridad de endpoints, desde antivirus hasta prevención de fugas de datos.
	La Consola de administración debe incluir un panel con un resumen visual en tiempo real para comprobar el estado de seguridad	Exigido	Cumple	Proporciona un panel visual en tiempo real	Cumple	Incluye un panel que muestra el estado de seguridad en tiempo real, visualmente intuitivo.
	Deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los ordenadores que necesitan atención	Exigido	Cumple	Ofrece filtros predefinidos para facilitar la gestión	Cumple	Ofrece filtros que identifican los dispositivos que requieren atención inmediata.
	Deberá mostrar los ordenadores administrados de acuerdo con los criterios de categoría (detalles del estado del equipo, detalles sobre la actualización, detalles de avisos y errores, detalles del antivirus, etc.), y ordenar los equipos en consecuencia	Exigido	Cumple	Clasifica los dispositivos administrados según criterios definidos	Cumple	Ordena los equipos según el estado de actualización, antivirus, alertas, etc.

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Actualizar de forma automática las directivas de seguridad cuando un equipo se mueve de un grupo a otro	Exigido	Cumple	Actualiza las políticas de seguridad automáticamente cuando un dispositivo cambia de grupo	Cumple	Las políticas de seguridad se actualizan automáticamente cuando un equipo cambia de grupo.
	Grabar un registro de auditoría seguro que supervise la actividad en la consola de administración para el cumplimiento de regulaciones, auditorías de seguridad, análisis y solución de problemas forenses	Exigido	Cumple	Graba un registro de auditoría seguro para cumplir con las normativas	Cumple	Mantiene un registro de auditoría detallado que ayuda a cumplir con normativas y análisis forenses.
	Deberá permitir exportar el informe de registros de auditoría en formatos CSV y PDF	Exigido	Cumple	Exporta los registros en formatos CSV y PDF	Cumple	Los registros de auditoría pueden exportarse en CSV y PDF para cumplir con auditorías.
	Debe contener varios informes para el análisis y control de los usuarios y endpoints. Los informes se deben dividir, como mínimo, en informes de: eventos, usuarios, control de aplicaciones, periféricos y web, indicando todas las funciones solicitadas para los endpoints	Exigido	Cumple	Ofrece varios informes detallados sobre usuarios y dispositivos	Cumple	Incluye varios informes para el control de eventos, usuarios, aplicaciones, y más.
	Permitir la ejecución manual de todos estos informes, así como la programación y envío automático por correo electrónico en los formatos CSV y PDF	Exigido	Cumple	Permite la programación y envío de informes automáticos	Cumple	Los informes se pueden programar para ser enviados automáticamente en CSV y PDF.
	Debe realizar envío automático de alertas críticas mediante correo electrónico a los administradores	Exigido	Cumple	Envía alertas automáticas por correo	Cumple	Envía automáticamente notificaciones por correo electrónico cuando ocurren eventos críticos.
	Detalle de usuarios activos, inactivos o desprotegidos, así como detalles de los mismos	Exigido	Cumple	Proporciona informes detallados de usuarios activos, inactivos o desprotegidos	Cumple	Permite generar informes que muestran el estado de los usuarios y dispositivos, incluyendo si están protegidos o no.
Capacidad de generación de informes	Detalle de los ordenadores que están activos, inactivos o desprotegidos, así como detalles de las exploraciones y alertas en los ordenadores	Exigido	Cumple	Informa sobre equipos activos, inactivos y desprotegidos	Cumple	La consola muestra el estado de los dispositivos y sus eventos de protección.
	Detalle de los periféricos permitidos o bloqueados, así como detalles de dónde y cuándo se utilizó cada periférico	Exigido	Cumple	Monitorea y controla los dispositivos periféricos conectados	Cumple	Genera informes sobre los periféricos utilizados, bloqueados y cuándo se usaron.

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Detalle de las principales aplicaciones bloqueadas y los servidores / usuarios que intentaron acceder a ellas Detalle de las aplicaciones permitidas que fueron accedidas con mayor frecuencia y los servidores / usuarios que las acceden Detalle de los servidores / usuarios que intentaron acceder a aplicaciones bloqueadas con mayor frecuencia y las aplicaciones que ellos intentaron acceder Detalle de todas las actividades disparadas por reglas de fuga de información.	Exigido	Cumple	Muestra los intentos de acceso a aplicaciones bloqueadas Informa sobre las aplicaciones más usadas Informa sobre los intentos de acceso no autorizados Monitorea las actividades relacionadas con fuga de información	Cumple	La consola registra y permite generar informes detallados sobre aplicaciones bloqueadas, intentos de acceso, y actividades de prevención de fuga de información.
Idiomas	Inglés (predeterminado) Portugués Alemán Francés Italiano Español Japonés Chino (tradicional y simplificado)	Exigido	Cumple	Soporta varios idiomas, incluidos español, japonés, y chino	Cumple	Admite múltiples idiomas, incluyendo: Inglés, Portugués, Alemán, Francés, Italiano, Español, Japonés, Chino (tradicional y simplificado)
Opciones de corrección de problemas	Proteger el dispositivo con la opción de inicio de una exploración	Exigido	Cumple	Permite iniciar una exploración de protección	Cumple	La consola permite iniciar una exploración manual en cualquier dispositivo para protección inmediata.
	Forzar una actualización en ese momento	Exigido	Cumple	Permite forzar actualizaciones inmediatas	Cumple	Se puede forzar una actualización del software y las definiciones de virus en tiempo real.
	Ver los detalles de los eventos ocurridos	Exigido	Cumple	Proporciona información detallada sobre los eventos y alertas de seguridad, incluyendo el historial de acciones	Cumple	Los administradores pueden revisar en detalle los eventos de seguridad en la consola.
	Ejecutar la comprobación completa del sistema	Exigido	Cumple	El sistema permite ejecutar una exploración completa del sistema para verificar cualquier amenaza presente	Cumple	Es posible ejecutar una verificación exhaustiva del sistema desde la consola.
	Forzar el cumplimiento de una nueva política de seguridad	Exigido	Cumple	El producto permite forzar una actualización inmediata en los dispositivos administrados	Cumple	Se pueden aplicar políticas de seguridad inmediatamente a los dispositivos.

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Mover el equipo a otro grupo	Exigido	Cumple	Proporciona información detallada sobre los eventos y alertas de seguridad, incluyendo el historial de acciones	Cumple	Los dispositivos pueden reorganizarse en diferentes grupos de administración.
	Borrar el equipo de la lista	Exigido	Cumple	El sistema permite ejecutar una exploración completa del sistema para verificar cualquier amenaza presente	Cumple	La consola permite eliminar dispositivos de la lista de gestión.
	El agente antivirus debe proteger computadoras portátiles, escritorios y servidores en tiempo real, bajo demanda o programado para detectar, bloquear y limpiar todos los virus, troyanos, gusanos y spyware. En Windows, el agente también debe detectar PUA, adware y spyware. En Windows, el agente también debe detectar PUA, adware y comportamiento sospechoso.	Exigido	Cumple	El agente de Kaspersky Next EDR Optimum protege dispositivos (portátiles, escritorios y servidores) en tiempo real contra virus, troyanos, gusanos, spyware y aplicaciones potencialmente no deseadas (PUA)	Cumple	El agente de Sophos ofrece protección en tiempo real, bajo demanda o programada, detectando y eliminando virus, troyanos, gusanos, spyware y PUA.
	Además del control de amenazas, el mismo agente (al menos Windows) debe proporcionar control de dispositivos, control de aplicaciones, control web y prevención de fuga de información (DLP).	Exigido	Cumple	Kaspersky proporciona control de dispositivos, aplicaciones, navegación web, y prevención de fuga de información (DLP)	Cumple	Además de la protección antivirus, proporciona control de dispositivos, aplicaciones, web y prevención de fuga de datos (DLP).
Características básicas del agente de protección	Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido	Exigido	Cumple	El producto incluye la capacidad de detección proactiva de malware mediante análisis de comportamiento antes de la ejecución	Cumple	Utiliza análisis de comportamiento para detectar malware desconocido antes de que se ejecute.
	Debe realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque	Exigido	Cumple	El sistema realiza verificaciones en tiempo real de todos los archivos accedidos, incluyendo durante el arranque	Cumple	Todos los archivos accedidos se verifican en tiempo real, incluso durante el arranque del sistema.
	Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA)	Exigido	Cumple	Kaspersky realiza la limpieza automática de elementos maliciosos y aplicaciones potencialmente indeseables	Cumple	El agente elimina automáticamente amenazas y PUA detectadas.
	Debe proteger las funciones críticas en los navegadores de Internet (Safe Browsing)	Exigido	Cumple	El sistema protege las funciones críticas del navegador mediante Safe Browsing, garantizando una navegación segura	Cumple	Protege las funciones críticas en los navegadores frente a amenazas online.

Abg. Nathalia Abril Vega Pérez
Profesional Administrativa
Secretaría General
ANTSV

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos	Exigido	Cumple	Kaspersky permite la autorización de detecciones maliciosas y la exclusión de determinados archivos, directorios y procesos del escaneo	Cumple	Permite autorizar detecciones y excluir archivos o directorios específicos de los escaneos.
	Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo virus, spyware, troyanos, gusanos, adware y aplicaciones potencialmente no deseadas (PUA)	Exigido	Cumple	Kaspersky permite el monitoreo y control de dispositivos extraíbles como USB, redes inalámbricas y otros periféricos	Cumple	El agente integra protección contra una amplia gama de amenazas (virus, spyware, troyanos, adware, etc.).
	Posee la funcionalidad de protección contra el cambio de la configuración del agente, impidiendo a los usuarios, incluyendo el administrador local, reconfigurar, deshabilitar o desinstalar componentes de la solución de protección	Exigido	Cumple	El control de dispositivos permite asignar permisos de solo lectura, completo o bloqueo según las políticas de seguridad	Cumple	Impide que usuarios, incluidos administradores locales, modifiquen, deshabiliten o desinstalen el agente sin autorización.
	Debe tener un mecanismo contra la desinstalación del endpoint por el usuario y cada dispositivo deberá tener una contraseña única, no siendo autorizadas soluciones con una contraseña que funcione en todos los dispositivos	Exigido	Cumple	El sistema admite el control de varios tipos de dispositivos, incluyendo discos duros externos, USB, CD, DVD, Bluetooth, entre otros	Cumple	Cada dispositivo tiene una contraseña única para evitar desinstalaciones no autorizadas.
	Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de los componentes de protección	Exigido	Cumple	El sistema permite monitorear e impedir que los usuarios ejecuten o instalen aplicaciones no autorizadas que puedan afectar la productividad o el rendimiento de la red	Cumple	Se puede configurar una contraseña para permitir la reconfiguración o desinstalación local del agente.
	Ser capaz de aplicar un análisis adicional, inspeccionando finamente el comportamiento de los códigos durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.	Exigido	Cumple	Utiliza análisis de comportamiento avanzado para detectar amenazas que se manifiestan durante la ejecución de aplicaciones. Este análisis permite identificar comportamientos sospechosos, como desbordamientos de búfer y otras actividades anómalas en tiempo real.	Cumple	Realiza un análisis detallado del comportamiento del código para detectar actividad sospechosa, como desbordamientos de búfer.
	Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits	Exigido	Cumple	El producto ofrece protección contra ataques que explotan vulnerabilidades en navegadores web, previniendo la ejecución de exploits	Cumple	El agente previene los ataques de vulnerabilidades de navegador a través de web exploits.

Alejandro R. Solís Zena
Jefe Dpto. de Patrimonio
ANTSV

Lic. Jan Daniel Vallejos Tanitwald
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Debe permitir el monitoreo y el control de dispositivos extraíbles en los equipos de los usuarios, como dispositivos USB, periféricos de la propia estación de trabajo y redes inalámbricas, aplicando estas políticas tanto para usuarios como para dispositivo	Exigido	Cumple	Soporta la monitorización y control de dispositivos extraíbles como USB, redes inalámbricas, y periféricos en los equipos de los usuarios, permitiendo aplicar políticas tanto a nivel de dispositivo como de usuario	Cumple	Monitorea y controla dispositivos como USB y redes inalámbricas, aplicando políticas de seguridad a nivel de usuario y dispositivo.
	El control de dispositivos debe estar al nivel de permiso, sólo lectura o bloqueo	Exigido	Cumple	Ofrece un control detallado de dispositivos, permitiendo aplicar políticas de seguridad que incluyen diferentes niveles de permisos.	Cumple	Ofrece control granular sobre dispositivos externos, permitiendo establecer permisos de lectura, escritura o bloqueo.
	Los siguientes dispositivos deben ser, como mínimo, administrados: HD (hard disks) externos, pendrives USB, almacenables removibles seguras, CD, DVD, Blu-ray, floppy drives, interfaces de red inalámbrica, módems, bluetooth, infrarrojo, MTP (Media Transfer Protocol) y PTP (Picture Transfer Protocol) como cámaras digitales	Exigido	Cumple	Proporciona un control completo sobre una amplia gama de dispositivos conectados a los equipos	Cumple	Soporta la administración de dispositivos como discos duros externos, USB, y otros medios removibles, incluyendo MTP y PTP.
	Control de aplicaciones para monitorear e impedir que los usuarios ejecuten o instalen aplicaciones que puedan afectar la productividad o el rendimiento de la red	Exigido	Cumple	Incluye un control de aplicaciones que permite a los administradores monitorear en tiempo real las aplicaciones instaladas y ejecutadas en los dispositivos de la red	Cumple	Monitorea e impide la ejecución de aplicaciones no autorizadas que puedan afectar la red.
	Capacidad de reconocer y bloquear automáticamente las aplicaciones en los clientes basándose en la huella digital (hash) del archivo.	Exigido	Cumple	Kaspersky reconoce y bloquea automáticamente las aplicaciones en función de la huella digital (hash) de los archivos	Cumple	Reconoce y bloquea aplicaciones no autorizadas basándose en su hash.
	Actualización automática de la lista de aplicaciones que se pueden controlar, permitiendo aplicaciones específicas o las categorías específicas de aplicaciones que pueden ser liberadas o bloqueadas	Exigido	Cumple	El sistema actualiza automáticamente las listas de aplicaciones permitidas o bloqueadas, según las políticas de seguridad establecidas	Cumple	La lista de aplicaciones controladas se actualiza automáticamente, permitiendo la clasificación y bloqueo.
	Detectar aplicaciones controladas cuando los usuarios acceden, con las opciones de permitir y alertar o bloquear y alertar	Exigido	Cumple	Kaspersky detecta aplicaciones controladas, permitiendo o bloqueando el acceso según las políticas, y genera alertas correspondientes	Cumple	Detecta cuando los usuarios acceden a aplicaciones y ofrece opciones de permitir, bloquear y alertar.

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Debe contar con prevención de intrusión en el host (HIPS), que monitoree el código y bloques de código que pueden comportarse de forma maliciosa antes de ser ejecutados	Exigido	Cumple	El sistema incluye prevención de intrusiones en el host (HIPS), monitoreando bloques de código que podrían ser maliciosos antes de ejecutarse	Cumple	Monitorea el comportamiento del código para detectar actividad maliciosa antes de la ejecución.
	Control de acceso a sitios web por categoría	Exigido	Cumple	Permite el control de acceso a sitios web basándose en categorías predefinidas, lo que ayuda a gestionar la navegación de los usuarios y bloquear el acceso a sitios inapropiados o que representen un riesgo para la seguridad	Cumple	Controla el acceso web por categoría, permitiendo restringir sitios inapropiados.
	El Control Web debe controlar el acceso a sitios inapropiados, con al menos 14 categorías de sitios inadecuados. También debe permitir la creación de listas blancas y listas negras.	Exigido	Cumple	El sistema incluye control web con al menos 14 categorías de sitios no deseados o inapropiados. Además, permite a los administradores crear listas blancas y negras para personalizar el acceso a sitios específicos, de acuerdo con las políticas de seguridad de la organización	Cumple	Ofrece al menos 14 categorías de sitios web para filtrar y permite crear listas blancas y negras.
	La aplicación de políticas de control web, debe contar con capacidad de horarios.	Exigido	Cumple	Permite configurar políticas de control web que se pueden aplicar en horarios específicos, lo que facilita el control del acceso web según los periodos laborales o las necesidades de la empresa	Cumple	Permite aplicar políticas de control web basadas en horarios.
	Debe poseer protección de fugas o pérdida de datos sensibles en el mismo agente de protección, considerando su contenido, además de la posibilidad de evaluar la extensión del archivo y múltiples destinos	Exigido	Cumple	El sistema ofrece protección contra fugas de datos sensibles (Data Loss Prevention - DLP) integrado en el mismo agente de protección. Puede detectar y bloquear la transferencia de datos confidenciales basándose en el contenido, la extensión del archivo y los múltiples destinos posibles, garantizando que la información no se filtre a lugares no autorizados	Cumple	Previene la fuga de datos confidenciales al evaluar el contenido y los destinos.
	Permitir la identificación de información confidencial, como números de pasaporte u otra información personal identificable y / o información confidencial, incluso si los documentos no se han clasificado correctamente, utilizando CCL (Lista de control de contenido)	Exigido	Cumple	Permite identificar información confidencial, incluyendo números de pasaporte, datos personales identificables (PII), y otros tipos de datos sensibles, incluso si no están correctamente clasificados, utilizando listas de control de contenido (CCL) para su protección	Cumple	Reconoce información personal como números de pasaporte, aun si no está clasificada correctamente, usando CCL.

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Posibilitar el bloqueo, sólo registrar el evento en la Consola de administración, o preguntar al usuario si él o ella realmente quiere transferir el archivo identificado como sensible	Exigido	Cumple	El sistema permite bloquear automáticamente la transferencia de archivos sensibles, registrar el evento en la consola de administración, o preguntar al usuario si realmente desea transferir el archivo identificado como sensible. Esto ofrece flexibilidad en la gestión de incidentes relacionados con la fuga de información	Cumple	Permite bloquear, registrar o solicitar confirmación al usuario sobre la transferencia de información sensible.
	Soportar agregar reglas propias de contenido con un asistente proporcionado para este propósito	Exigido	Cumple	Permite a los administradores definir reglas personalizadas para el control de contenido. Estas reglas pueden crearse utilizando un asistente que guía a los usuarios a través del proceso, lo que facilita la personalización de políticas de seguridad para adaptarse a necesidades específicas de la organización	Cumple	Permite crear reglas personalizadas de contenido para gestionar la seguridad.
	Capacidad de autorizar, bloquear y confirmar el movimiento de información sensible y en todos los casos, grabar la operación realizada con las principales informaciones de la operación	Exigido	Cumple	El sistema ofrece la capacidad de autorizar, bloquear o confirmar el movimiento de información sensible. Cada operación realizada es registrada en la consola de administración, asegurando un seguimiento detallado de todas las acciones relacionadas con datos confidenciales y garantizando el cumplimiento de las políticas de seguridad de la empresa	Cumple	Autoriza, bloquea o confirma el movimiento de datos sensibles y graba la operación.
	El Agente para servidores debe contemplar monitoreo de integridad de archivos, al menos en servidores Windows.	Exigido	Cumple	Incluye monitoreo de la integridad de archivos en servidores Windows, lo que permite detectar cualquier cambio no autorizado en archivos críticos del sistema. Esto es clave para garantizar la seguridad y el cumplimiento en entornos de servidores	Cumple	Ofrece monitoreo de integridad de archivos, al menos en servidores Windows, detectando cambios no autorizados.

Lic. Natalia de la Vega Pérez
Profesional Administrativa
Secretaría General
ANTSV

Alejandro R. Solís Zena
Jefe Dpto. de Patrimonio
ANTSV

Lic. Juan Daniel Vallejos Tambaril
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Números de tarjetas de crédito	Exigido	Cumple	Puede identificar números de tarjetas de crédito como parte de su funcionalidad de prevención de pérdida de datos (DLP). Utiliza listas de control de contenido (CCL) preconfiguradas para detectar información financiera confidencial	Cumple	Identifica los números de tarjetas de crédito en documentos y comunicaciones, protegiendo este tipo de información crítica contra posibles fugas o robos de datos.
	Números de cuentas bancarias	Exigido	Cumple	El sistema permite detectar y proteger números de cuentas bancarias utilizando sus capacidades DLP, ayudando a evitar la fuga de este tipo de información sensible	Cumple	El sistema reconoce los números de cuentas bancarias, bloqueando o registrando intentos de transferencia o acceso no autorizado, ayudando a prevenir fraudes financieros.
Identificadores de listas CCL preconfiguradas	Números de pasaportes	Exigido	Cumple	Incluye la identificación de números de pasaportes, garantizando que los datos de identificación personal (PII) sean protegidos contra transferencias no autorizadas	Cumple	Identifica y protege información relacionada con números de pasaportes, brindando seguridad en transacciones y documentos que contengan estos datos personales.
	Direcciones	Exigido	Cumple	El sistema puede identificar direcciones dentro de los archivos monitoreados, lo que permite aplicar políticas de seguridad y evitar la filtración de datos personales	Cumple	Intercepta cualquier fuga potencial de direcciones físicas o electrónicas, lo que protege la información personal de los usuarios y reduce el riesgo de exposición.
	Números de teléfono	Exigido	Cumple	Los números de teléfono están cubiertos por las capacidades de identificación de datos personales y sensibles de Kaspersky, ayudando a prevenir su transferencia no autorizada	Cumple	Identifica y controla la transferencia de números de teléfono, previniendo su divulgación no autorizada y protegiendo la privacidad de los usuarios.
	Lista de correos electrónicos	Exigido	Cumple	El sistema permite identificar direcciones de correo electrónico como parte de las listas de control de contenido (CCL), asegurando que esta información sea gestionada de manera segura y bloqueada si es necesario	Cumple	Protege contra la fuga de listas de correos electrónicos, bloqueando o alertando cuando esta información se comparte sin autorización, lo que ayuda a prevenir el robo de identidades y correos no deseados.
Medios para control de datos	Adjunto en el cliente de correo electrónico (al menos Outlook y Outlook Express)	Exigido	Cumple	Permite el control de adjuntos enviados o recibidos a través de clientes de correo electrónico, incluyendo Outlook y Outlook Express. Esto es parte de sus capacidades de prevención de fuga de información (DLP), que monitorean y bloquean el envío de información sensible por correo electrónico	Cumple	Sophos intercepta y controla adjuntos enviados por correo a través de clientes como Outlook, detectando archivos que puedan contener datos sensibles.

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Adjunto en el navegador (al menos IE, Firefox y Chrome)	Exigido	Cumple	El sistema monitorea y controla los adjuntos que se suben o descargan desde navegadores como Internet Explorer, Firefox y Chrome, lo que ayuda a prevenir la transferencia no autorizada de datos sensibles a través de la web	Cumple	Monitorea y bloquea archivos adjuntos en navegadores web, protegiendo contra la fuga de datos a través de formularios y plataformas online.
	Adjunto en el cliente de mensajería instantánea (al menos Skype)	Exigido	Cumple	Incluye control sobre los adjuntos enviados a través de clientes de mensajería instantánea, como Skype. Esto garantiza que los archivos confidenciales no sean transferidos sin la debida autorización	Cumple	Controla archivos enviados a través de plataformas de mensajería como Skype, asegurando que no se transmitan datos confidenciales sin autorización.
	Adjunto a dispositivos de almacenamiento (al menos USB, CD / DVD)	Exigido	Cumple	Monitorea y controla la transferencia de archivos adjuntos a dispositivos de almacenamiento, tales como USB, CD, y DVD, bloqueando o registrando estas acciones según las políticas de seguridad aplicadas	Cumple	Bloquea o monitorea la transferencia de archivos hacia medios de almacenamiento externo, como USBs o CDs, protegiendo la información al impedir la copia no autorizada.
	Protección de amenazas de día 0 a través de tecnología de deep learning (signature less).	Exigido	Cumple	Utiliza tecnología de deep learning para detectar y proteger contra amenazas de día cero sin depender de firmas de virus. Esto le permite identificar y bloquear amenazas nuevas y desconocidas de manera proactiva	Cumple	Utiliza tecnología de deep learning sin depender de firmas tradicionales para detectar amenazas de día cero.
Funcionalidad de detección proactiva de reconocimiento de nuevas amenazas	Funcionalidad de detección de amenazas desconocidas que están en memoria	Exigido	Cumple	El sistema es capaz de detectar amenazas desconocidas en la memoria mediante análisis de comportamiento, lo que le permite identificar ataques que intentan ejecutarse directamente en la memoria de los dispositivos	Cumple	Detecta y neutraliza malware desconocido que opera exclusivamente en la memoria.
	Capacidad de detección, y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria	Exigido	Cumple	Tiene la capacidad de detectar y bloquear de manera proactiva keyloggers y otros tipos de malware desconocido, incluyendo ataques de día cero, mediante el análisis del comportamiento de los procesos en memoria. Este enfoque asegura que las amenazas se bloqueen antes de causar daño	Cumple	Analiza el comportamiento de los procesos en memoria para bloquear keyloggers y malware desconocido.

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Capacidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria	Exigido	Cumple	El producto detecta y bloquea troyanos, gusanos (worms) y otras formas de malware basándose en el comportamiento de los procesos en memoria, sin depender de firmas, lo que lo convierte en una solución efectiva para contrarrestar amenazas avanzadas	Cumple	Detecta y bloquea troyanos, gusanos y otros malware basándose en la actividad de procesos.
	No debe requerir descarga de firmas de ningún tipo.	Exigido	Cumple	Ofrece protección sin necesidad de descargar firmas, utilizando análisis de comportamiento y tecnologías avanzadas como el aprendizaje profundo para identificar amenazas nuevas y desconocidas	Cumple	No depende de la descarga continua de firmas, utilizando análisis de comportamiento y tecnologías avanzadas.
	Capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.	Exigido	Cumple	Analiza el comportamiento de los procesos al ser ejecutados, complementando la exploración programada para detectar posibles amenazas de manera proactiva, ofreciendo así una capa adicional de protección	Cumple	Evalúa el comportamiento de nuevos procesos en tiempo real, complementando los escaneos programados.
	Análisis forense de lo sucedido, para entender cuál fue la causa raíz del problema con el detalle de los procesos y sub-procesos ejecutados, la lectura y escritura de archivos y de las claves de registro.	Exigido	Cumple	El sistema proporciona análisis forense detallado para entender la causa raíz de los incidentes de seguridad. Esto incluye la revisión de los procesos y subprocesos ejecutados, así como las operaciones de lectura y escritura en archivos y claves de registro, facilitando la investigación y la solución de problemas	Cumple	Proporciona análisis forense detallado de incidentes, rastreando procesos y subprocesos ejecutados, lecturas escrituras de archivos, y modificaciones de claves de registro.
	Bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).	Exigido	Cumple	Detecta y bloquea amenazas potencialmente no deseadas (PUA), incluyendo aquellas que no han sido previamente identificadas, protegiendo el sistema contra posibles amenazas ocultas	Cumple	Bloquea amenazas desconocidas potencialmente sospechosas, como PUA.
	Generación de excepciones ante falsos positivos.	Exigido	Cumple	El sistema permite la generación de excepciones para gestionar falsos positivos, lo que garantiza que los administradores puedan ajustar las políticas de seguridad sin comprometer la operatividad	Cumple	Permite definir excepciones para reducir los falsos positivos, manteniendo la precisión en la protección.

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Disponer de capacidad de protección contra ransomware basada en comportamiento	Exigido	Cumple	Ofrece protección avanzada contra ransomware basada en el comportamiento de las aplicaciones. Esto le permite identificar y bloquear actividades sospechosas que puedan estar relacionadas con ataques de ransomware, incluso antes de que ocurran	Cumple	Usa análisis de comportamiento para detectar y bloquear actividades de ransomware en tiempo real.
	Disponer de capacidad de remediación de la acción de encriptación de los ransomware	Exigido	Cumple	El sistema incluye capacidades de remediación para revertir los efectos del ransomware. Puede detener la encriptación en curso y recuperar los archivos que hayan sido encriptados por el ransomware	Cumple	Incluye herramientas de remediación que revierten la acción de encriptación del ransomware.
Funcionalidad de protección contra ransomware	Capacidad de detección del cifrado malicioso de forma local o remoto	Exigido	Cumple	Es capaz de detectar intentos de cifrado malicioso tanto localmente como en sistemas remotos, lo que permite bloquear la propagación del ransomware en la red y evitar que el cifrado afecte más dispositivos	Cumple	Detecta actividades de cifrado tanto en el entorno local como remoto.
	Debe poseer protección anti-ransomware para el sector de booteo (master boot record).	Exigido	Cumple	Incluye protección anti-ransomware para el sector de booteo (MBR), lo que garantiza que los ataques dirigidos a esta área crítica del sistema sean bloqueados antes de que puedan ejecutarse	Cumple	Ofrece protección específica contra ransomware que intenta modificar el MBR.
	Debe restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.	Exigido	Cumple	El producto tiene la capacidad de restaurar automáticamente los archivos encriptados por ransomware, asegurando una recuperación rápida sin la intervención manual del usuario	Cumple	Sophos puede restaurar automáticamente archivos cifrados por ransomware.
	Debe informar a la consola todo el detalle del incidente análisis de causa raíz sin la necesidad de instalar otro agente o dispositivo en la red	Exigido	Cumple	Proporciona un análisis detallado del incidente directamente en la consola de administración, sin necesidad de instalar agentes adicionales. El sistema incluye un análisis de causa raíz que permite a los administradores entender cómo ocurrió el ataque y tomar medidas preventivas	Cumple	Proporciona un análisis detallado del incidente sin la necesidad de instalar agentes adicionales en la red, centralizando la información en la consola.

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidades conocidas o de día cero	Exigido	Cumple	Tiene la capacidad de bloquear ataques que explotan vulnerabilidades conocidas y de día cero. Utiliza análisis de comportamiento y tecnologías avanzadas para identificar y detener amenazas antes de que puedan aprovechar dichas vulnerabilidades	Cumple	Utiliza tecnología anti-exploit que protege contra vulnerabilidades conocidas y de día cero sin necesidad de actualizaciones de firmas. Detecta y bloquea técnicas de explotación antes de que puedan aprovecharse de las vulnerabilidades, brindando protección proactiva contra ataques nuevos y desconocidos.
	Mitigación de inyección de códigos en procesos	Exigido	Cumple	El sistema mitiga los ataques que intentan inyectar código malicioso en procesos en ejecución. Kaspersky detecta y bloquea estas inyecciones, impidiendo que el código malicioso comprometa el sistema	Cumple	La solución incluye mitigaciones que previenen la inyección de código en procesos legítimos. Esto se logra a través de la monitorización y control de procesos en tiempo real, bloqueando cualquier intento de inyección maliciosa que pueda comprometer el sistema.
Protección contra Vulnerabilidades y técnicas de explotación	Protección contra robo de credenciales	Exigido	Cumple	Ofrece protección específica contra técnicas de robo de credenciales, bloqueando los intentos de acceder a información sensible como contraseñas y datos de autenticación. Esto incluye la detección de keyloggers y otros métodos utilizados para robar credenciales	Cumple	Ofrece protección específica contra técnicas utilizadas para robar credenciales, como el acceso no autorizado a la memoria del sistema y herramientas de volcado de credenciales. Esto ayuda a prevenir que los atacantes obtengan información sensible de inicio de sesión.
	Protección contra malware escondido en aplicaciones legítimas (code cave)	Exigido	Cumple	El sistema es capaz de detectar malware oculto dentro de aplicaciones legítimas, una técnica conocida como "code cave". Esta capacidad garantiza que incluso si un malware está incrustado en un software aparentemente confiable, será detectado y bloqueado	Cumple	Utiliza análisis de comportamiento y técnicas avanzadas para detectar malware que se oculta dentro de aplicaciones legítimas, conocido como "code cave". Esto permite identificar y neutralizar amenazas que intentan evadir la detección al integrarse en software confiable.
	Evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.	Exigido	Cumple	Evita que los procesos maliciosos migren de un proceso a otro, una técnica comúnmente utilizada para evadir la detección. Esto se logra mediante un monitoreo constante de los procesos en ejecución y bloqueando los intentos de migración	Cumple	La solución impide que procesos maliciosos migren o se inyecten en otros procesos, evitando que el malware se oculte o escale sus privilegios. Esto se logra mediante la monitorización de las actividades de los procesos y el bloqueo de comportamientos sospechosos.

Abg. Natalia de la Vega Pérez
Profesional Administrativa
Secretaría General
ANTSV

Alejandro H. Solís Zena
Jefe Dpto. de Patrimonio
ANTSV

Lic. Juan Daniel Vallejos Tanibarki
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Evitar obtener escalamiento de privilegios	Exigido	Cumple	El sistema impide los intentos de escalamiento de privilegios, que es cuando un atacante intenta obtener mayores permisos en un sistema para realizar acciones no autorizadas. Kaspersky bloquea estos intentos al detectar comportamientos sospechosos relacionados con la elevación de privilegios	Cumple	Detecta y bloquea intentos de escalamiento de privilegios, donde el malware intenta obtener niveles de acceso más altos en el sistema. Esto protege contra ataques que buscan controlar completamente el dispositivo afectado.
	Modificación de las claves de registro para la ejecución de código arbitrario	Exigido	Cumple	Previene la modificación no autorizada de las claves de registro que podría permitir la ejecución de código arbitrario. Esta protección es fundamental para evitar que los atacantes modifiquen configuraciones críticas del sistema para ejecutar su propio código malicioso	Cumple	La solución protege las claves de registro críticas del sistema contra modificaciones no autorizadas que podrían permitir la ejecución de código arbitrario. Monitorea cambios en el registro y bloquea actividades que puedan comprometer la integridad del sistema.
	Enforce Data Execution Prevention	Exigido	Cumple	Aplica Data Execution Prevention (DEP), lo que impide que el código se ejecute desde regiones de memoria no ejecutables, una técnica clave para prevenir la ejecución de código malicioso	Cumple	Bloquea la ejecución de código en áreas de memoria no autorizadas, asegurando que solo los datos legítimos se ejecuten.
	Mandatory Address Space Layout Randomization	Exigido	Cumple	El sistema implementa ASLR obligatorio, que ayuda a mitigar los ataques al randomizar la ubicación de áreas clave de memoria, dificultando la explotación de vulnerabilidades	Cumple	Randomiza la ubicación de áreas clave en la memoria para impedir que los atacantes predigan su localización.
Detección y protección de las siguientes técnicas de explotación	Bottom-up ASLR	Exigido	Cumple	Incluye Bottom-up ASLR, una técnica que refuerza la seguridad al aplicar ASLR desde las direcciones de memoria más bajas, complicando los intentos de explotación	Cumple	Protege contra ataques que intentan predecir la ubicación de secciones clave del sistema.
	Null Page (Null Deference Protection)	Exigido	Cumple	El sistema previene ataques que intentan aprovechar la página nula en memoria, bloqueando los intentos de desreferenciación nula (Null Dereference) que podrían llevar a la ejecución de código malicioso	Cumple	Impide la explotación de la página nula en la memoria, utilizada por algunos ataques.

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Heap Spray Allocation Dynamic Heap Spray	Exigido	Cumple	Detecta y bloquea ataques de "heap spraying", donde el atacante intenta llenar el heap con datos maliciosos para sobrescribir áreas críticas de la memoria El producto incluye protección contra técnicas de "Dynamic Heap Spray", mitigando los intentos de explotación que utilizan esta técnica avanzada para manipular el heap en tiempo de ejecución	Cumple	Bloquea las técnicas de heap spraying, donde los atacantes inundan la memoria con código malicioso.
	Stack Pivot	Exigido	Cumple	Detecta y previene intentos de "stack pivoting", una técnica utilizada para redirigir el flujo de ejecución de un programa hacia código malicioso en la pila	Cumple	Evita que los atacantes redirijan el flujo de ejecución hacia áreas no deseadas en la memoria.
	Stack Exec (MemProt)	Exigido	Cumple	Evita que el código malicioso se ejecute en la pila mediante la protección de la memoria de ejecución en la pila	Cumple	Protege contra la ejecución de código malicioso en la pila de ejecución.
	Stack-based ROP Mitigations (Caller) Branch-based ROP Mitigations (Hardware Assisted)	Exigido	Cumple	El sistema mitiga los ataques basados en ROP (Return-Oriented Programming), protegiendo contra la manipulación de la pila mediante técnicas avanzadas de mitigación basadas en el retorno del programa (Caller) Utiliza mitigaciones basadas en el uso de hardware para proteger contra ataques ROP basados en la ramificación de código, una técnica que aprovecha las instrucciones de hardware para aumentar la seguridad	Cumple	Mitiga técnicas de retorno orientado a programación (ROP), impidiendo que los atacantes encadenen instrucciones maliciosas.
	Structured Exception Handler Overwrite (SEHOP)	Exigido	Cumple	El sistema implementa SEHOP (Protección contra la sobrescritura del manejador de excepciones estructuradas), lo que impide la explotación de vulnerabilidades a través de la modificación de los manejadores de excepciones en Windows	Cumple	Bloquea intentos de sobreescribir el manejador de excepciones estructuradas.

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Import Address Table Filtering (IAF)	Exigido	Cumple	Utiliza el filtrado de la tabla de direcciones de importación (IAF) para bloquear la ejecución de código malicioso mediante la manipulación de las direcciones de importación de bibliotecas	Cumple	Protege contra la manipulación de la tabla de direcciones de importación, comúnmente utilizada en exploits.
	Load Library	Exigido	Cumple	El sistema protege contra la explotación de vulnerabilidades a través de la carga maliciosa de bibliotecas mediante el uso de técnicas seguras para la carga dinámica de librerías (DLL)	Cumple	Monitorea y controla la carga de bibliotecas dinámicas (DLL) para impedir la ejecución no autorizada.
	Reflective DLL Injection	Exigido	Cumple	Protege contra la inyección reflexiva de DLLs, una técnica en la que un atacante intenta inyectar y ejecutar una DLL maliciosa en un proceso legítimo sin escribir en el disco	Cumple	Bloquea intentos de inyección de DLL reflexiva, una técnica de malware avanzada.
	Shellcode	Exigido	Cumple	El producto detecta y bloquea el uso de shellcode, un tipo de código que los atacantes suelen utilizar para tomar control de un sistema durante la explotación de vulnerabilidades	Cumple	Detecta y bloquea intentos de ejecutar shellcode malicioso en la memoria.
	VBScript God Mode	Exigido	Cumple	Protege contra técnicas como el "VBScript God Mode", una vulnerabilidad que permite a los atacantes ejecutar comandos arbitrarios con permisos elevados	Cumple	Protege contra vulnerabilidades relacionadas con VBScript, que permiten a los atacantes ejecutar código arbitrario.
	Wow64	Exigido	Cumple	El sistema incluye protección contra exploits que se aprovechan de la capa de compatibilidad Wow64, utilizada para ejecutar aplicaciones de 32 bits en sistemas de 64 bits	Cumple	Mitiga ataques en sistemas Windows que ejecutan aplicaciones de 32 bits en un entorno de 64 bits.
	Syscall	Exigido	Cumple	Monitorea y bloquea intentos de exploits que utilizan llamadas directas al sistema (syscalls) para evitar mecanismos de seguridad del sistema operativo	Cumple	Bloquea intentos de acceder directamente a funciones del sistema operativo mediante llamadas al sistema.

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Hollow Process	Exigido	Cumple	Detecta y bloquea técnicas de "Hollow Process", donde los atacantes reemplazan el código de un proceso legítimo con código malicioso para evadir la detección	Cumple	Impide la técnica de inyección de procesos huecos, donde un atacante reemplaza un proceso legítimo por uno malicioso.
	DLL Hijacking	Exigido	Cumple	Previene los ataques de secuestro de DLLs (DLL Hijacking), donde los atacantes intentan cargar una DLL maliciosa en lugar de una legítima para comprometer un sistema	Cumple	Protege contra el secuestro de DLL, donde se cargan versiones maliciosas de bibliotecas en lugar de las legítimas.
	Squiblydoo Applocker Bypass	Exigido	Cumple	El sistema protege contra la técnica "Squiblydoo", que permite a los atacantes eludir las políticas de AppLocker y ejecutar código malicioso mediante aplicaciones legítimas de Windows	Cumple	Bloquea ataques que eluden las restricciones de Applocker.
	APC Protection (Double Pulsar / AtomBombing)	Exigido	Cumple	Incluye protección contra ataques que utilizan APCs (Asynchronous Procedure Calls), como Double Pulsar y AtomBombing, técnicas avanzadas que permiten a los atacantes inyectar código malicioso en otros procesos	Cumple	Protege contra ataques avanzados como Double Pulsar y AtomBombing que manipulan la ejecución de procesos.
	Process Privilege Escalation	Exigido	Cumple	El sistema bloquea los intentos de escalamiento de privilegios, donde los atacantes intentan obtener mayores permisos en el sistema para realizar acciones maliciosas	Cumple	Detecta y bloquea intentos de escalamiento de privilegios, impidiendo que los atacantes obtengan control total del sistema.
	Soportar máquinas con arquitectura de 32 bits y 64 bits	Exigido	Cumple	Es compatible con máquinas que utilizan arquitecturas tanto de 32 bits como de 64 bits, permitiendo su despliegue en una amplia variedad de entornos de trabajo	Cumple	Es compatible con arquitecturas de 32 bits y 64 bits, asegurando protección en ambos tipos de sistemas.
Despliegue Agente	El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Mac OS X 10.10 en adelante,	Exigido	Cumple	El cliente de Kaspersky Next EDR Optimum es compatible con macOS, incluyendo versiones a partir de OS X 10.10 en adelante, lo que asegura que los usuarios de equipos Mac puedan implementar el software en sus sistemas	Cumple	Es compatible con macOS, pero la compatibilidad generalmente comienza desde macOS 10.12 (Sierra) en adelante. Es posible que no sea totalmente compatible con Mac OS X 10.10 (Yosemite) y 10.11 (El Capitan). Aunque se da esta situación, en la institución no se tiene equipos con sistema operativo OS

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Windows 7 en adelante	Exigido	Cumple	El producto es totalmente compatible con estaciones de trabajo que utilicen Windows 7 en adelante, cubriendo versiones más modernas de Windows y garantizando su instalación en la mayoría de los entornos empresariales	Cumple	Es compatible con Windows 7 y versiones posteriores, incluyendo Windows 8, 8.1 y 10, brindando protección completa en estas plataformas.
	El cliente para instalación en servidores debe ser compatible con los sistemas operativos Windows server 2008 en adelante.	Exigido	Cumple	Puede instalarse en servidores que ejecuten Windows Server 2008 y versiones posteriores, lo que le permite proteger infraestructuras de servidor tanto antiguas como modernas	Cumple	Sophos Intercept X es compatible con Windows Server 2008 R2 y versiones posteriores. Sin embargo, la compatibilidad con Windows Server 2008 (sin R2) puede ser limitada o no estar garantizada. Aunque se da esta situación, en la institución no se tiene equipos con sistema operativo Windows Server 2008 (sin R2)
	CentOS 6/7	Exigido	Cumple	Es compatible con las versiones 6 y 7 de CentOS, permitiendo la protección en tiempo real en este sistema operativo	Cumple	Es compatible con CentOS, brindando protección en tiempo real para las versiones 6 y 7 de este sistema operativo.
	Debian 9	Exigido	Cumple	El sistema ofrece soporte para Debian 9, lo que permite el despliegue y protección en tiempo real en esta distribución de Linux	Cumple	El soporte incluye Debian 9, garantizando protección en tiempo real.
	Oracle Linux 6/7	Exigido	Cumple	Es compatible con Oracle Linux en sus versiones 6 y 7, proporcionando protección en tiempo real para sistemas basados en esta plataforma	Cumple	Soporta Oracle Linux en sus versiones 6 y 7, con protección en tiempo real.
Sistemas Operativos Linux soportados (en tiempo real)	Red Hat Enterprise Linux 6/7	Exigido	Cumple	Ofrece soporte completo para Red Hat Enterprise Linux (RHEL) versiones 6 y 7, garantizando protección en tiempo real en entornos empresariales que usen esta distribución	Cumple	Las versiones 6 y 7 de Red Hat son compatibles con el agente de Sophos.
	SUSE 12/15	Exigido	Cumple	El producto es compatible con SUSE Linux Enterprise en las versiones 12 y 15, ofreciendo protección y monitoreo en tiempo real	Cumple	Ofrece protección en tiempo real para SUSE en las versiones 12 y 15.

Ana Natalia de la Vega Pérez
Profesional Administrativa
Secretaría General
ANTSV

Alejandro R. Solís Zona
Jefe Dpto. de Patrimonio
ANTSV

Lic. Juan Daniel Vallejos Tanlwald
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

Ítem	Descripción	Exigencia	Empresa SEGEL S.A.	Observaciones	Empresa ITCS	Observaciones
	Ubuntu 14.16/18	Exigido	Cumple	Es compatible con Ubuntu en las versiones 14, 16 y 18, asegurando que los usuarios que utilicen esta distribución puedan proteger sus sistemas en tiempo real	Cumple	También incluye soporte para Ubuntu en las versiones 14, 16 y 18, proporcionando una cobertura completa para este sistema.
Vigencia	24 meses contando a partir de la fecha de emisión del certificado de recepción satisfactoria.	Exigido	Cumple	Consta en la oferta económica	Cumple	Consta en la oferta económica
Soporte	Deberá incluir 70 horas de servicio de soporte in situ o remoto por parte del oferente adjudicado, durante el periodo de vigencia de las licencias. Deploy de antivirus y herramientas en equipos clientes. Configuración de reglas y políticas de la herramienta. Capacitación y soporte sobre las herramientas implementadas al equipo técnico de la ANTSV.	Exigido	Cumple	Exigible con la capacidad técnica cumplida	Cumple	Exigible con la capacidad técnica cumplida
Autorización	El oferente deberá contar con una autorización apostillada del fabricante para presentar la oferta. A su vez, el oferente deberá estar debidamente autorizado por el fabricante para prestar servicio técnico.	Exigido	Cumple	Presenta el documento	Cumple	Presenta el documento

Ing. Natalia de la Vega Pérez
Profesional Administrativa
Secretaría General
ANTSV

Alejandro R. Solís Zena
Jefe Dpto. de Patrimonio
ANTSV

Lic. Juan Daniel Vallejos Tanhwald
Jefe de Unidad Técnica de Proyectos
DNLCAT - ANTSV

10) MARGEN DE PREFERENCIA

MARGEN DE PREFERENCIA PARA PRODUCTOS NACIONALES
Margen de Preferencia para productos nacionales se aplicará el margen de preferencia nacional de conformidad a la legislación vigente. La acreditación de Origen Nacional del Producto, en el marco de proceso de contratación, será a través del Certificado de Origen Nacional.
No aplica, debido a que ambas empresas son de origen extranjero.

11) CONCLUSIÓN FINAL:

*Analizadas todas las documentaciones, el Comité Evaluador ha constatado que la oferta presentada por la firma **SEGEL S.A.** y la firma **ITCS S.A.** cumplen a cabalidad con los requisitos establecidos en el Pliego de Bases y Condiciones, por lo cual podrán ser consideradas como oferta elegible.*

RESUMEN DE LAS DOCUMENTACIONES ANALIZADAS.

Oferentes	Documentos sustanciales	Capacidad Financiera	Experiencia Requerida	Capacidad Técnica	Precio Ofertado
SEGEL S.A.	CUMPLE	CUMPLE	CUMPLE	CUMPLE	Gs. 36.548.120
ITCS S.A.	CUMPLE	CUMPLE	CUMPLE	CUMPLE	Gs. 42.820.190
ARIVOIR S. A	NO CUMPLE	-	-	-	Gs. 43.400.000

12) RECOMENDACIÓN DEL COMITÉ

Por todo lo expuesto, este Comité de Evaluación recomienda:

*1° **ADJUDICAR** el Proceso Licitatorio **ANTSV N.° 04/2024 LICITACIÓN DE MENOR CUANTÍA NACIONAL** "SERVICIO DE SUSCRIPCIÓN DE SOFTWARE ANTIVIRUS" - ID NRO. 444175 a la empresa **SEGEL S.A.**, por el precio unitario de **Gs. 522.116** y por el monto total de **Gs. 36.548.120**. Debido a que cumple con todos los requisitos sustanciales y formales de acuerdo al análisis realizado por este comité de evaluación de conformidad al Pliego de Bases y Condiciones del llamado y por ofertar el precio más bajo.*

En prueba de conformidad, se da por terminado el acto, firmando los Miembros como acostumbran a hacerlo en dos ejemplares de un mismo tenor y a un solo efecto, en fecha 08 de octubre de 2024 a las 14:00 horas.

Abg. Nathalia De la Vega Pérez	Sr. Alejandro Ramon Solís Zena	Lic. Jun Daniel Vallejos T.
Profesional Administrativa	Jefe de Dpto.	Jefe de Dpto.
Secretaria General	Departamento de Patrimonio	Unidad Técnica de Proyectos DNLCAT