Licitación Pública Nacional N° 02/2024
"Adquisición de Licencias Antivirus" Plurianual ID N° 446.119

INFORME DE EVALUACIÓN DE OFERTAS

En la ciudad de Asunción, capital de la República del Paraguay, a los 18 días del mes de octubre del año dos mil veinte y cuatro, se inicia el proceso de evaluación de las ofertas del llamado a **Licitación Pública Nacional N° 02/2024 "Adquisición de Licencias Antivirus" Plurianual ID N° 446.119** cuyo miembros del Comité de Evaluación están constituido según Resolución N° 1381/2024 de fecha 13 de agosto de 2.024 por el Sr. Emilio Peralta por la Dirección TICS, la Abg. Silvia Bogado Armoa por la Dirección de Asesoría Jurídica y el Abg. Atilio Gómez por la Dirección Financiera, sobre la base de las disposiciones contenidas en la Ley 7021/22 "DE CONTRATACIONES PÚBLICAS", sus modificaciones y reglamentación vigente.

1. ANTECEDENTES:

a. El llamado a **Licitación Pública Nacional N° 02/2024 "Adquisición de Licencias Antivirus" Plurianual ID N° 446.119** fue solicitado por Memorando DITC N° 153/2024 de la Dirección de TICS.
b. La aprobación del llamado por Resolución D.G N° 1381/2024 de fecha 13 de agosto de 2.024 **Licitación Pública Nacional N° 02/2024 "Adquisición de Licencias Antivirus" Plurianual ID N° 446.119**
c. En fecha 01 de julio del 2024, mediante Dictamen Técnico Jurídico UOC N° 32/2024, se dictamina la elaboración del Precio **Licitación Pública Nacional N° 02/2024 "Adquisición de Licencias Antivirus" Plurianual ID N° 446.119**
d. El presente llamado es Ad referéndum
e. Forma de adjudicación: **por Total**

2. CRITERIO DE EVALUACIÓN Y MÉTODO DE PRESENTACIÓN DE OFERTAS

En virtud de la naturaleza de la contratación, de conformidad a lo establecido en el inciso b) del Artículo 52 "Evaluación, subsanabilidad y rechazo de las ofertas" de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas", en el Artículo 75 "Procedimiento de Evaluación" numeral 2) Evaluación basada únicamente precio, del Decreto Reglamentario N° 2264/2024 y a lo dispuesto en el Pliego de Bases y Condiciones (PBC); se ha establecido el **precio como único criterio de evaluación.**

3. ACTA DE APERTURA DE OFERTA

Conforme se desprende del Acta de Apertura de Oferta de fecha 17 de octubre de 2024, se ha procedido a la apertura del sobre de acuerdo con el siguiente detalle:

1	80070889-0	Corporation Sekiura S.A.C.E.I	info@sekiura.com.py

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Peralta
Ministerio de la Defensa Pública

Oferentes	Formulario de Oferta debidamente Firmado	Documento que acredita la identidad y la representación del firmante de la oferta	Declaración Jurada del Artículo 40	Garantía de Mantenimiento de Oferta
Corporation Sekiura S.A.C.E.I	SI	SI	SI	Moneda de la oferta: Guaraníes Monto total de la oferta: 792.281.000 Tipo de Garantía: POLIZA DE SEGURO Empresa Aseguradora: Royal Seguros S.A. Monto total asegurado Gs.: 42.500.000 Vigencia de la Póliza: De 17/10/2024 a 15/04/2025, 180 días

Oferentes	Páginas foliadas	Constancia del SIPE N°	Muestras	Inscripto
Corporation Sekiura S.A.C.E.I	32	1819165	NO	Registro Proveedor

4. OBSERVACIONES EN EL ACTO DE APERTURA DE OFERTA

No hubo observaciones

5. VERIFICACIÓN DEL CUMPLIMIENTO DE LOS REQUISITOS DE CARÁCTER SUSTANCIAL

Posteriormente, se ha procedido a la verificación del cumplimiento de la oferta respecto a la presentación de las documentaciones básicas de carácter sustancial, de conformidad a lo establecido en el Artículo 79 del del Decreto Reglamentario N° 2264/2024 y demás disposiciones que rigen las Contrataciones Públicas, observándose lo siguiente:

OFERENTE	Formulario de Oferta. Listado de precio	Garantía de Mantenimiento	Escritura Pública de constitución	Poderes del firmante	Fotocopia C.I del firmante de la Oferta	Constancia de RUC
Corporation Sekiura S.A.C.E.I	Cumple	Cumple	Cumple	No aplica	Cumple	Cumple

Verificadas las documentaciones de carácter sustancial: Formulario de oferta y la lista de precios debidamente llenados y firmados; Garantía de mantenimiento de oferta debidamente extendida, documentos que acreditan la existencia del oferente; los documentos que demuestren las facultades del firmante de la oferta para comprometer al oferente, y documentos que la DNCP determine como sustanciales, se verifica que las firmas oferentes **Corporation Sekiura S.A.C.E.I** cumplen con las documentaciones de carácter sustancial.

Abg. Atilio A. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Perelli
Ministro de la Defensa Pública

6. REGISTRO DE PROVEEDORES DEL ESTADO

De conformidad con lo establecido en el Artículo 22 de la Ley N° 7021/2022, en el Artículo 33 del Decreto Reglamentario N° 2264/2024 y los Artículos 10 y 39 de la Resolución DNCP N° 3801/2023, este Comité de Evaluación deja constancia que la empresa **Corporation Sekiura S.A.C.E.I** obra en la base de datos del módulo "Registro de Proveedores del Estado" del Sistema de Información de las Contrataciones Públicas (SICP).

7. CAPACIDAD LEGAL

De conformidad con lo dispuesto en el Artículo 21 – "Prohibiciones y limitaciones para presentar propuestas y contratar" de la Ley N° 7021/22 "De Suministro y Contrataciones Públicas", y en el apartado "Requisitos de Calificación" de la sección "Requisitos de participación y criterios de evaluación" del Pliego de Bases y Condiciones (PBC), se ha procedido a solicitar informe a la Dirección de Gestión de Talento Humano por Nota UOC N° 529/2024 remitida en fecha 21 de octubre de 2024, sobre aspectos legales que guardan relación con la oferta presentada, acompañando el Anexo de Listado del Oferente con los datos personales de cada miembro identificado que forma parte del oferente de la presente convocatoria

Por Memorándum D.G.T.H N° 3352/2024 recibida en fecha 22 de octubre de 2024, la Dirección de Gestión de talento Humano remite los solicitado en Nota UOC N° 529/2024 donde se puede apreciar que ninguno de los miembros declarados en el "*Formulario de Declaración de Personal*" forman parte del Ministerio de la Defensa Pública.

7.1 VERIFICACIÓN DEL REGISTRO DE PROVEEDORES INHABILITADOS (ART. 23 LEY 7021/22)

Este Comité de Evaluación ha procedido a verificar si la empresa oferente (Persona Jurídica y física), e incluyendo a las personas indicadas en el "Formulario de Declaración de Personal" (Artículo 21, Ley N° 7021/2022), se encuentran inhabilitadas para contratar con el Estado a través del Registro de Proveedores Inhabilitados disponible en el Sistema de Información de las Contrataciones Públicas (SICP) de la Dirección Nacional de Contrataciones Públicas (DNCP), observándose lo siguiente:

Oferente	Ruc	Inhabilitado (SI/NO)
Corporation Sekiura S.A.C.E.I	80070889-0	No

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Peralta
Ministro de la Defensa Pública

Verificación según declaración jurada de personas

OFERENTE	Corporation Sekiura S.A.C.E. I	
Nombre	**Nélida Rafaela Aponte de Fischer**	**Ingrid Fischer Aponte**
Numero de cedula	397.359	4.204.194
Registro de plantel de funcionarios de la convocante	No existe registro en el MDP	No existe registro en el MDP
Registro funcionarios Sistema Nacional de Recurso Humano (SINARH)	No existe registro en el SINARH	No existe registro en el SINARH

No habiendo registros en el Listado de funcionarios de Ministerio de la Defensa Publica ni en el SINARH, se deja constancia que no se verifica impedimentos legales. Teniendo en cuenta que los oferentes **Corporation Sekiura S.A.C.E.I** han presentado en el formulario de oferta y en el formulario de declaración de Miembros la declaración jurada de no hallarse comprendidos en las prohibiciones y limitaciones establecidas en el Art. 21 "Prohibiciones y limitaciones para presentar propuestas y contratar" de la Ley 7021/22 y no habiendo elementos para desacreditar el documento este comité considera.

8 -ERRORES ARITMÉTICOS

Luego de verificar la oferta de los oferentes participantes, se verifica que no se presentan errores aritméticos por lo cual se persigue con la evaluación.

9- CERTIFICADO DE PRODUCTO Y EMPLEO NACIONAL

De conformidad a lo establecido en la Ley N° 4558/2011 de fecha 11 de diciembre del año 2011 "*QUE ESTABLECE MECANISMOS DE APOYO A LA PRODUCCIÓN Y EMPLEO NACIONAL, A TRAVÉS DE LOS PROCESOS DE CONTRATACIONES PUBLICAS", la Ley N° 6575/2020 de fecha 18 de noviembre de 2020 "QUE MODIFICA EL ARTICULO 2° DE LA LEY N° 4558/2011 "QUE ESTABLECE MECANISMOS DE APOYO A LA PRODUCCIÓN Y EMPLEO NACIONAL, A TRAVÉS DE LOS PROCESOS DE CONTRATACIONES PÚBLICAS" y la Circular DNCP N° 09/24,* este Comité de Evaluación constatando que las empresas oferente no realizaron el trámite correspondiente para su emisión debido a que los productos ofrecidos no son de industria nacional, por lo que no se aplica ningún margen de preferencia.

10- TABLA COMPARATIVA DE PRECIOS DE LA OFERTA

De conformidad con la disposición contenida en el numeral 2., en su punto 2.1.2 del Artículo 75 del Decreto N° 2264/2024, se ha procedido a la verificación de la planilla de precios presentada por la empresa oferente que ha cumplido con la documentación de carácter sustancial, no observándose errores aritméticos según se expone en el siguiente cuadro:

Abg. Atilio R. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa4 [illegible]

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Duarte
Ministerio de la Defensa Pública

Licitación: 446119 - Adquisición de Licencias (Antivirus)

Grupo 1 - Adquisición de Licencias (Antivirus) Contrato Abierto: No, Abastecimiento Simultaneo: No

Ítem	Código Catálogo	Descripción	Atributos	Cantidad	Precio Unitario (IVA Incluido)	Precio Total	Caracteristicas
1	43233205-002	Renovación de Licencia para Antivirus Kaspersky	Unidad de medida: Unidad Presentación: UNIDAD	1.813	437.000	792.281.000	marca: Kaspersky fabricante: Kaspersky procedencia: Reino Unido
TOTAL						792.281.000	

Habiéndose verificado la planilla de precios presentada por el oferente, se procedió a seleccionar las ofertas evaluadas, de acuerdo a lo dispuesto en el numeral 2., en su punto 2.1.3 del Artículo 75 del Decreto Reglamentario N° 2264/2024 según el siguiente cuadro:

Oferente	Precio ofertado
Corporation Sekiura S.A.C.E.I	792.281.000

Se selecciona provisoriamente a la única oferta, **Corporation Sekiura S.A.C.E.I** ***que será analizada en detalle para verificar su cumplimiento con otros requisitos de la contratación***

11. SOLICITUD DE ACLARACIÓN DE LA OFERTA Y LA RESPUESTA DEL OFERENTE

Se deja constancia que el pedido de documentos a la empresa oferente fue practicado en virtud a lo dispuesto en el Art. 77 del Decreto Reglamentario N° 2264/2024 y en conformidad expresa a lo estipulado en el inciso a) del Formulario de Oferta publicado en el Sistema de Información de las Contrataciones Públicas (SICP), el cual establece taxativamente cuanto sigue: ***"a)…Reconocemos que la dirección de correo electrónico declarada, será el medio para la recepción de las comunicaciones, notificaciones, aclaraciones y consultas que la convocante realice durante la evaluación de ofertas…"***.

Así también, se considera pertinente traer a colación lo indicado en el inciso b) del Formulario de Oferta publicado en el Sistema de Información de las Contrataciones Públicas (SICP), el cual expone textualmente: ***"b) Entendemos que los plazos se computarán desde el día siguiente a la fecha de remisión de las comunicaciones, notificaciones, aclaraciones y consultas, sin necesidad de contar con acuse de recibo…"***.

- **Se solicito por Nota UOC N° 530/2024 al oferente *Corporation Sekiura S.A.C.E.I* el siguiente documento:**

1. El proveedor deberá presentar autorización del fabricante, y en caso de representante o distribuidor deberán demostrar que los mismos están autorizados como tal por el Fabricante.
2. Demostrar la experiencia en provisión de ADQUISICION Y/O RENOVACION DE LICENCIAS ANTIVIRUS con facturaciones de venta, contratos y/o recepciones finales,

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pú...

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Fiscal General
Ministerio de la Defensa Pública

por un monto equivalente al 50 % como mínimo del monto total ofertado en el presente procedimiento de contratación, dentro de los últimos 3(tres) años (2021, 2022 y 2023) en Instituciones públicas y/o privadas, se tendrá en cuenta la suma de las facturaciones hasta llegar al monto solicitado, si con un periodo se llega al porcentaje requerido se dará por cumplido, no siendo necesario presentar documentaciones por cada periodo.

3. Balance General y Cuadro de Resultados de los años 2021, 2022, 2023 para contribuyentes de IRACIS/IRE, acorde a las normas contables y a los modelos establecidos en las Normativas Vigentes de la Dirección Nacional de Ingresos Tributarios(www.dnit.gov.py).
4. Formulario de liquidación de impuesto de IRP o IRPC o su equivalente según la nueva reglamentación tributaria de los años 2021, 2022, 2023
5. Presentar copia del certificado que avale que se cuenta con como mínimo con 1 ingeniero certificado con las certificaciones avanzadas del producto.
6. Presentar copia del certificado que avale que se cuenta con como mínimo con 1 técnico con certificaciones de cifrado
7. Presentar copia del certificado que avale que se cuenta con por lo menos 1 técnico con certificaciones en protección de servidores de correo antispam
8. Presentar DECLARACIÓN JURADA DE ESTAR O NO ESTAR INCURSO/A EN CAUSALES DE LOS DEBERES DE ABSTENCIÓN EN CASO DE CONFLICTOS DE INTERESES EN RELACIÓN A FUNCIONARIOS PÚBLICOS, de conformidad con el formulario estándar – sección formularios.

El oferente **Corporation Sekiura S.A.C.E.I** presento en fecha y forma lo solicitado

12- VERIFICACIÓN DE LOS CRITERIOS DE EVALUACIÓN

12.1 Verificación de Documentos de Carácter Formal Corporation Sekiura S.A.C.E.I

EMPRESA OFERENTE – PERSONA JURÍDICA	**Corporation Sekiura S.A.C.E. I**
Documentos Requeridos	
Certificado de Cumplimiento con la Seguridad Social.	*Cumple*
Certificado de Producto y Empleo Nacional, emitido por el MIC.	*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*
Autorización de Fabricante	
El proveedor deberá presentar autorización del fabricante, y en caso de representante o distribuidor deberán demostrar que los mismos están autorizados como tal por el Fabricante.	*Cumple*
Requisitos documentales para evaluar la Experiencia Requerida	
Demostrar la experiencia en provisión de ADQUISICION Y/O RENOVACION DE LICENCIAS ANTIVIRUS con facturaciones de venta, contratos y/o recepciones finales, por un monto equivalente al 50 % como mínimo del monto total ofertado en el presente procedimiento de contratación, dentro de los últimos 3(tres) años (2021, 2022 y 2023) en Instituciones públicas y/o privadas, se tendrá en cuenta la suma de las facturaciones hasta llegar al monto solicitado, si con un periodo se llega al porcentaje	*Cumple*

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto 6
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

requerido se dará por cumplido, no siendo necesario presentar documentaciones por cada periodo.	

13- Capacidad Financiera

13.1 Para contribuyente de IRACIS/IRE GENERAL, IRPC/IRE SIMPLE, IRP e IVA GENERAL. AÑOS 2021, 2022, 2023.-

- ✓ Para contribuyentes de IRACIS/IRE GENERAL: Deberá cumplir con el siguiente parámetro de los años (2021, 2022, 2023). -

a) Ratio de Liquidez: activo corriente / pasivo corriente Deberá ser igual o mayor que 1, en promedio, en los 3 últimos años (2021, 2022, 2023).

b) Endeudamiento: pasivo total / activo total No deberá ser mayor a 0,80 en promedio, e n los 3 últimos años (2021, 2022,2023).

c) Rentabilidad: Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital. El promedio en los últimos 3 años (2021, 2022, 2023), no deberá ser negativo.

OFERENTE:	Corporation Sekiura SACEI					
Balance General	**2021**	**2022**	**2023**	**PROMEDIO**	**PARÁMETRO A CUMPLIR**	**OBS.**
Activo Corriente	3.658.505.966	5.926.595.553	6.790.123.192			
Pasivo Corriente	2.521.355.043	4.166.605.289	3.225.777.695			
Ratio de Liquidez	**1,451**	**1,422**	**2,105**	**1,66**	>= 1	**CUMPLE**
Pasivo Total	2.521.355.043	4.166.605.289	3.225.777.695			
Activo Total	6.198.999.052	10.158.501.507	6.198.999.052			
Ratio de Endeudamiento	**0,41**	**0,41**	**0,52**	**0,45**	<= 0,80	**CUMPLE**
Utilidad Neta	878.444.279	2.314.252.009	834.522.065			
Capital	2.600.000.000	2.600.000.000	2.600.000.000			
Ratio de Rentabilidad	**0,34**	**0,89**	**0,32**	**0,52**	No Deberá ser Negativo	**CUMPLE**

13.2 Requisitos documentales para la evaluación de la capacidad financiera

Balance General y Cuadro de Resultados de los años 2021, 2022, 2023 para contribuyentes de IRACIS/IRE, acorde a las normas contables y a los modelos establecidos en las Normativas Vigentes de la Dirección Nacional de Ingresos Tributarios(www.dnit.gov.py).	Cumple
Formulario de liquidación de impuesto de IRP o IRPC o su equivalente según la nueva reglamentación tributaria de los años 2021, 2022, 2023	Cumple

Abg. Atilio A. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Peralta
Ministerio de la Defensa Pública

14- Análisis de los precios ofertados

Los criterios de evaluación para los precios ofertados establecidos en la Resolución DNCP N° 454/2024 de fecha 15 de febrero de 2024 fueron aplicados para la evaluación correspondiente, constatándose que los precios ofertados no se encuentran fuera de los rangos.

Licitación: 446119 - Adquisición de Licencias (Antivirus)

Grupo 1 - Adquisición de Licencias (Antivirus) Contrato Abierto: No, Abastecimiento Simultaneo: No

Ítem	Código Catálogo	Descripción	Atributos	Cantidad	Precio Unitario (IVA Incluido)	Precio Total
1	43233205-002	Renovación de Licencia para Antivirus Kaspersky	Unidad de medida: Unidad Presentación: UNIDAD	1.813	437.000	792.281.000
TOTAL						792.281.000

Precio Promedio Referencial	Variación
794.396.771	0,27%

13- CAPACIDAD TÉCNICA

Documento requerido	
Presentar copia del certificado que avale que se cuenta con como mínimo con 1 ingeniero certificado con las certificaciones avanzadas del producto.	Cumple
Presentar copia del certificado que avale que se cuenta con como mínimo con 1 técnico con certificaciones de cifrado.	Cumple
Presentar copia del certificado que avale que se cuenta con por lo menos 1 técnico con certificaciones en protección de servidores de correo antispam	Cumple
El proveedor debe proporcionar una copia de 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 copia del certificado que avale ser Canal Platinum de la Marca ofertada, para garantizar el buen servicio y respaldo del soporte local.	Cumple

13.1 Otros Documentos solicitados en el PBC

Presentar DECLARACIÓN JURADA DE ESTAR O NO ESTAR INCURSO/A EN CAUSALES DE LOS DEBERES DE ABSTENCIÓN EN CASO DE CONFLICTOS DE INTERESES EN RELACIÓN A FUNCIONARIOS PÚBLICOS, de conformidad con el formulario estándar – sección formularios.	Cumple

Se solicito al área Técnica Dirección de TICS según Nota UOC 570/2024 de fecha 25 de octubre de 2024 un informe, a fin de dar cumplimiento de la capacidad técnica

En fecha 28 de octubre la Dirección de TICS remite su informe donde expresan los siguiente: **Anexo 3**

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Peralta
Ministro de la Defensa Pública

Oferentes que cumplen con lo requerido en el Pliego de Bases y Condiciones

De conformidad con lo establecido en el numeral 2 en su punto 2.1 del Artículo 75 "Procedimiento de evaluación" del Decreto Reglamentario N° 2264/2024, y teniendo en cuenta los criterios analizados ut supra, el Comité de Evaluación deja constancia que la empresa **Corporation Sekiura S.A.C.E.I** cumple con el suministro de la documentación básica de carácter sustancial, con la capacidad legal, con la contestación de la solicitud de aclaración, con las especificaciones técnicas, capacidad técnica, financiera y con la experiencia, conforme a lo requerido en el Pliego de Bases y Condiciones. –

14-RECOMENDACIÓN DE ADJUDICACIÓN

Por tanto, atendiendo a los criterios de evaluación expresados precedentemente, al Sistema de Adjudicación por Total contemplado en el Sistema de Información de las Contrataciones Públicas (SICP), con ID N° 446.119, se recomienda la ADJUDICACIÓN, salvo mejor parecer de la Máxima Autoridad, a la siguiente empresa:

- **Corporation Sekiura S.A.C.E.I con RUC 80070889-0,** por un monto total **Gs. 792.281.000.-** (guaraníes Setecientos noventa y dos millones doscientos ochenta y un Mil), incluido todos los impuestos

Sin otro punto que tratar se levanta la sesión a los 28 días del mes de octubre del año 2024, firmando los miembros del Comité de Evaluación.

Abg. Atilio Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Peralta
Defensa Pública

CONSIDERACIONES GENERALES.
SUITE DE SEGURIDAD Y PROTECCIÓN DE SOFTWARE PARA EMPRESAS. SERVIDOR DE ADMINISTRACIÓN Y CONSOLA ADMINISTRATIVA.

	Solución: Item N° 1 Antivirus Kaspersky NEXT EDR Optimum	cumple/no cumple
1	**Información General.**	
2	**Características Generales**	
2,1	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.	**cumple**
2,2	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.	**cumple**
2,3	La solución debe proteger endpoints y servers, sean estos Windows, Linux, macOS, así como también dispositivos móviles iOS y Android.	**cumple**
2,4	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.	**cumple**
2,5	La solución debe permitir la implementación de puntos de distribución en diferentes segmentos de red o ubicaciones geográficas de la organización que permita 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.	**cumple**
2,6	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	**cumple**
2,7	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;	**cumple**
2,8	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;	**cumple**
2,9	La solución debe contar con la capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto;	**cumple**
2,10	La solución debe disponer de la capacidad de importar la estructura de Active Directory para encontrar máquinas;	**cumple**

Abg. Atilio J. Gomez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

2,11	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;	**cumple**
2,12	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;	**cumple**
3	Proteccion para Endpoints, Consola de Administracion, Anti Spam y Reporting	**cumple**
3,1	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.	**cumple**
3,2	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).	**cumple**
3,3	Las 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	**cumple**
3,4	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	**cumple**
3,5	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	**cumple**
3,6	La solución debe permitir establecer una programación para el análisis, de manera que se pueda realizar de forma manual o según programación	**cumple**
3,7	La solución debe permitir analizar archivos compuestos de formatos ZIP, GZIP, BZIP, RAR, TAR, ARJ, CAB, LHA, JAR, ICE y otros archivos comprimidos	**cumple**
3,8	La solución debe permitir analizar archivos protegidos con contraseña	**cumple**
3,9	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	**cumple**
3,10	La solución debe analizar tráfico HTTP, HTTPS y FTP	**cumple**
3,11	La solución debe bloquear el tráfico HTTP que no cumple con los estándares RFC	**cumple**

Emilio Perali
Ministerio de la Defensa Pública

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

3,12	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 otras amenaza	cumple
3,13	La solución de protección frente a amenazas en el correo debe ser compatible con POP3, SMTP, IMAP y NNTP	cumple
3,14	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]	cumple
3,15	La solución debe incluir un componente de protección frente a amenazas en la red que monitoree el tráfico de red entrante en busca de actividad característica de los ataques de red	cumple
3,16	La solución debe bloquear la conexión de red con el equipo atacante	cumple
3,17	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	cumple
3,18	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.	cumple
3,19	La solución debe permitir seleccionar el protocolo y el puerto que se van a usar para la comunicación y permitir actividades de red específicas	cumple
3,20	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	cumple
3,21	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.	cumple
3,22	El componente de firewall de escritorio debe controlar la actividad de red de las aplicaciones en el equipo	cumple
3,23	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	cumple
3,24	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	cumple
3,25	El componente de firewall de escritorio debe controlar la actividad de la red sobre el protocolo seleccionado: TCP, UDP, ICMP, ICMPv6, IGMP y GRE	cumple

Abg. Atilio A. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

3,26	El componente de firewall de escritorio debe permitir seleccionar los adaptadores de red que pueden enviar o recibir paquetes de red	**cumple**
3,27	El componente de firewall de escritorio debe permitir restringir el control de los paquetes de red según su período de vida (TTL)	**cumple**
3,28	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	**cumple**
3,29	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	**cumple**
3,30	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	**cumple**
3,31	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	**cumple**
3,32	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)	**cumple**
3,33	La solución debe incluir un componente de protección AMSI diseñado para ser compatible con Antimalware Scan Interface de Microsoft	**cumple**
3,34	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	**cumple**
3,35	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	**cumple**
3,36	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	**cumple**
3,37	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	**cumple**
3,38	El componente de prevención de intrusiones en el host debe controlar el funcionamiento de las aplicaciones mediante el uso de derechos de las aplicaciones	**cumple**
3,39	Los derechos de las aplicaciones debe incluir los siguientes parámetros de acceso:	**cumple**

Abg. Atilio J. Gómez Ayala
Dpto. de Despacho
Ministerio de la Defensa Pública

Emilio Peralta
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Peralta
Ministerio de la Defensa Pública

	- Acceso a recursos del sistema operativo (por ejemplo, opciones de inicio automático y claves de registro)	**cumple**
	- Acceso a datos personales (como archivos y aplicaciones)	**cumple**
3,40	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	**cumple**
3,41	La solución debe incluir un componente de motor de reparación que le permita revertir las acciones realizadas por aplicaciones maliciosas en el sistema operativo	**cumple**
3,42	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:	**cumple**
	- Elimina los archivos ejecutables que el malware ha creado (en cualquier tipo de soporte, excepto unidades de red)	**cumple**
	- Elimina los archivos ejecutables creados por programas en los que el malware se ha infiltrado	**cumple**
	- Restaura los archivos que el malware ha modificado o eliminado	**cumple**
	- Elimina las claves del registro que el malware ha creado	**cumple**
	- No restaura las claves del registro que el malware ha modificado o eliminado	**cumple**
	- Finaliza los procesos iniciados por el malware	**cumple**
	- Finaliza los procesos en los que haya penetrado una aplicación maliciosa	**cumple**
	- No reanuda procesos que el malware haya suspendido	**cumple**
	- Bloquea la actividad de red del malware	**cumple**
	- Bloquea la actividad de red de los procesos en los que el malware se ha infiltrado.	**cumple**
3,43	La solución debe incluir un componente de control web que permita regular el acceso de los usuarios a los recursos web	**cumple**
3,44	El componente de control web debe permitir supervisar tráfico HTTP y HTTPS	**cumple**

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

3,45	El componente de control web debe permitir configurar el acceso a los sitios web a través de estos criterios:	**cumple**
	- Categorías de sitios web	**cumple**
	- Tipo de datos	**cumple**
	- Direcciones individuales	**cumple**
3,46	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	**cumple**
3,47	El componente de control web debe utilizar al menos los siguientes filtros:	**cumple**
	- Filtrar por contenido y tipo de datos	**cumple**
	- Filtrar por direcciones de recursos web	**cumple**
	- Filtrar por nombres de usuarios y grupos de usuarios	**cumple**
3,48	El componente de control web debe permitir seleccionar alguna de las siguientes acciones:	**cumple**
	- Permitir	**cumple**
	- Bloquear	**cumple**
	- Advertir	**cumple**
3,49	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	**cumple**
3,50	El componente de control de dispositivos debe controlar el acceso a los siguientes niveles:	**cumple**
	- Tipo de dispositivo	**cumple**
	- Bus de conexión	**cumple**
	- Dispositivos de confianza	**cumple**

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Emilio Peralta
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Peralta
Ministerio de la Defensa Pública

3,51	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	cumple
3,52	El componente de control de dispositivos debe permitir crear reglas del acceso para los siguientes tipos de dispositivo, mínimamente:	cumple
	- Discos duros	cumple
	- Unidades extraíbles (incluidas las unidades flash USB)	cumple
	- Disquetes	cumple
	- Unidades de CD/DVD	cumple
		cumple
	- Dispositivos portátiles (MTP)	cumple
	- Impresoras locales	cumple
	- Impresoras de red	cumple
	- Módems	cumple
	- Unidades de cinta	cumple
	- Dispositivos multifuncionales	cumple
	- Lectores de tarjetas inteligentes	cumple
	- Dispositivos Windows CE USB ActiveSync	cumple
	- Adaptadores de red externos	cumple
	- Bluetooth	cumple
	- Cámaras y escáneres	cumple
3,53	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.	cumple

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

3,54	La solución debe incluir un componente de control de aplicaciones que permita gestionar el inicio de aplicaciones en los equipos de los usuarios	**cumple**
3,55	El componente de control de aplicaciones debe permitir crear categorías de aplicaciones que se quieren gestionar	**cumple**
3,56	El componente de control de aplicaciones debe permitir crear reglas en la directiva para el grupo de administración	**cumple**
3,57	El componente de control de aplicaciones debe poder funcionar en dos modos:	**cumple**
	- 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.	**cumple**
	- 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.	**cumple**
3,58	El componente de control de aplicaciones debe crear una imagen propietaria de los programas que garantizan el funcionamiento normal del sistema operativo	**cumple**
3,59	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	**cumple**
3,60	La solución debe incluir características básicas de Endpoint Detection and Response (EDR)	**cumple**
3,61	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	**cumple**
3,62	La solución debe contar con la capacidad de mostrar toda la información disponible sobre la amenaza detectada	**cumple**
3,63	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.	**cumple**
3,64	La solución debe incluir una API abierta (OpenAPI) que permita personalizar escenarios operativos y tareas a través de la consola de gestión central	**cumple**
3,65	La solución debe incluir, dentro de su licenciamiento, la conexión a una infraestructura de servicios en la nube que brinde acceso a la base de conocimientos en línea del fabricante, que permita conocer la reputación de los archivos, los recursos web y aplicaciones, de manera que la solución de una respuesta más rápida a las amenazas, mejore el rendimiento de los componentes de protección y reduzca la probabilidad de falsas alarmas.	**cumple**

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Emilio Peralta
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Peralta
Ministerio de la Defensa Pública

3,66	La solución debe contar, dentro de su licenciamiento, con integración y acceso con un Portal de Inteligencia contra Amenazas, que permita consultar información sobre la reputación de archivos y URLs.	cumple
3,67	La solución debe ofrecer un proceso de recomendaciones de respuesta a alertas	cumple
3,68	La solución debe proveer información sobre el dispositivo protegido en el que se produce la alerta (por ejemplo, nombre del dispositivo, dirección IP, dirección MAC, lista de usuarios, sistema operativo, entre otros).	cumple
3,69	La solución debe proveer información sobre el objeto detectado.	cumple
3,70	La solución debe proveer información relacionada con los cambios en el registro asociados con la alerta.	cumple
3,71	La solución debe proveer información de historial de la presencia del archivo en el dispositivo.	cumple
3,72	La solución debe proveer información de las acciones de respuesta realizadas por la aplicación.	cumple
3,73	La solución debe ofrecer la posibilidad de aislar dispositivos de la red a petición (manualmente) o como una acción automática para responder a las amenazas detectadas, desde la consola de administración central sin intervención del usuario final.	cumple
3,74	La solución debe incluir una funcionalidad que permita obtener información sobre los dispositivos que se encuentren aislados de la red	cumple
3,75	La solución debe permitir establecer exclusiones de aislamiento de red. Es decir que las conexiones de red que cumplan las condiciones de la exclusión especificada no se bloquearán en los dispositivos después de que se active el aislamiento de red.	cumple
3,76	La solución debe incluir, dentro de su licenciamiento, un SandBox basado en Nube que permita detectar amenazas complejas en los equipos de los usuarios.	cumple
3,77	La solución debe permitir enviar automáticamente al Sandbox basado en Nube los archivos que es necesario analizar.	cumple
3,78	La solución debe permitir ver los informes de alertas detectadas por la tecnología de Sandbox basado en Nube.	cumple
3,79	La solución debe permitir crear tareas de Análisis de IoC con el fin de encontrar indicadores de compromiso en el dispositivo y realizar acciones de respuesta a la amenaza.	cumple
3,80	La solución debe permitir crear tareas de análisis de IoC grupal o local. Es decir que se permita ejecutar en un solo dispositivo o en varios de manera simultánea.	cumple

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

3,81	La solución debe permitir crear tareas de análisis de IoC de forma automática en respuesta a una amenaza detectada por el Sandbox basado en nube.	**cumple**
3,82	La solución debe permitir ejecutar una de las siguientes acciones de respuesta disponibles para los IoC detectados:	**cumple**
	- Aislar el dispositivo de la red.	**cumple**
	- Ejecutar análisis de áreas críticas.	**cumple**
	- Poner la copia en cuarentena y eliminar el objeto	**cumple**
		cumple
3,83	La solución debe incluir un componente de cifrado de datos que permita cifrar las carpetas y los archivos almacenados en las unidades locales y extraíbles, o las unidades extraíbles y los discos duros por completo, con el fin de minimizar el riesgo de filtraciones de información que se puede producir en caso de pérdida o robo del equipo portátil, unidad extraíble o disco duro, o cuando usuarios y aplicaciones no autorizados acceden a los datos	**cumple**
3,84	El componente de cifrado de datos debe utilizar el algoritmo de cifrado AES (del inglés "Advanced Encryption Standard") con sus variantes de cifrado "fuerte" (AES256) como la de cifrado "ligero" (AES56)	**cumple**
3,85	El componente de cifrado de datos debe ofrecer las siguientes características de protección de datos:	**cumple**
	- Cifrado de archivos en unidades locales del equipo	**cumple**
	- Cifrado de unidades extraíbles	**cumple**
	- Gestión de reglas de acceso de las aplicaciones a los archivos cifrados	**cumple**
	- Creación de paquetes cifrados	**cumple**
	- Cifrado de disco completo	**cumple**
3,86	El componente de cifrado de datos debe permitir realizar cifrado de disco completo con la tecnología de cifrado propietaria del fabricante	**cumple**
3,87	El componente de cifrado de datos debe ser compatible con los sistemas de archivos FAT32, NTFS y exFAT.	**cumple**
3,88	El componente de cifrado de datos debe ser capaz de continuar con las operaciones de cifrado de disco completo en caso que el equipo sea apagado o entre en estado de hibernación o suspensión	**cumple**

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Emilio Peralta
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

3,89	El componente de cifrado de datos debe permitir el uso de la tecnología de Single Sign-On (SSO) con el fin de iniciar sesión automáticamente en el sistema operativo utilizando las credenciales del agente de autenticación	cumple
3,90	El componente de cifrado de datos debe permitir gestionar el cifrado de Microsoft BitLocker desde la consola central	cumple
3,91	El componente de cifrado de datos debe incluir los siguientes estados de cifrado:	cumple
	- No cumple la directiva; cancelado por el usuario. El usuario ha cancelado el cifrado de datos.	cumple
	- No cumple la directiva debido a un error. Error de cifrado de datos; por ejemplo, falta una licencia.	cumple
	- Aplicando la directiva. Reinicio necesario. Cifrado de datos en curso en el equipo. Reinicie el equipo para completar el cifrado de datos.	cumple
	- No se ha especificado ninguna directiva de cifrado. El cifrado de datos está desactivado en la configuración de directiva.	cumple
	- No compatible. Los componentes de cifrado de datos no están instalados en el equipo.	cumple
	- Aplicando la directiva. El cifrado y el descifrado de datos está en curso en el equipo.	cumple
3,92	El componente de cifrado de datos debe permitir ver las estadísticas del cifrado en el dashboard de la solución	cumple
3,93	El componente de cifrado de datos debe proveer una utilidad de restauración que se pueda emplear para la recuperación de datos	cumple
3,94	El componente de cifrado de datos debe permitir la creación de un disco de rescate del sistema operativo que sirva cuando no se pueda acceder a un disco duro cifrado por alguna razón y el sistema operativo no se puede cargar	cumple
4	**Proteccion para Office 365**	cumple
4,1	La Solución de Seguridad debe integrarse con Microsoft Office 365 de manera nativa mediante Microsoft Office 365 API sin influir ni requerir cambios en los flujos de tráfico de correo electrónico.	cumple
4,2	La solución debe disponer de una consola de gestión que permita la configuración y administración multi-usuario de todas las capacidades ofertadas de manera integral, facilitando la gestión de la seguridad en Microsoft Office 365.	cumple
4,3	La solución no debe requerir cambio alguno en los registros MX de correo o en las aplicaciones de Microsoft Office 365 para su funcionamiento.	cumple

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Peralta
Ministerio de la Defensa Pública

4,4	La solución debe de validar de Spam, Phishing, Ransomware, BEC, amenazas conocidas y desconocidas en tiempo real para correos electrónicos entrantes, salientes y aquellos que fluyen internamente en la propia instancia de Microsoft Office 365.	**cumple**
4,5	La solucion debe utilizar heurística avanzada, aislamiento de procesos, aprendizaje automático y otras tecnologías de última generación para proteger a las empresas que utilizan Microsoft Exchange Online, Microsoft Teams, Microsoft OneDrive y Microsoft SharePoint Online contra el ransomware, archivos adjuntos maliciosos, spam, phishing, correos electrónicos que comprometen la seguridad de la empresa (BEC) y amenazas desconocidas.	**cumple**
4,6	La solución debe cumplir con el Reglamento General de Protección de Datos (RGDP) y protección de los datos.	**cumple**
4,7	La solución debe de contar con tecnologías de detección Anti-Spam, Anti-Phishing, Anti- Malware, Anti-Ransomware, Anti-BEC & capacidades de filtrado de contenido.	**cumple**
4,8	La solución debe de contar con tecnologías proactivas para la detección de amenazas avanzadas o de día 0.	**cumple**
4,9	La solución debe de contar con tecnologías de detección avanzadas para la detección y neutralización de amenazas del tipo Ransomware.	**cumple**
4,10	La solución debe disponer de capacidades de escaneo bajo demanda sobre buzones de correo pudiendo seleccionar.	**cumple**
	- Grupos de usuarios	**cumple**
	- Usuarios	**cumple**
	- Todos los usuarios	**cumple**
4,11	La solución debe poder clasificar los correos basura en dos categorías: Spam y correos masivos y poder definir las acciones a tomarse en cada uno de los casos.	**cumple**
4,12	La solución debe contar con capacidades de generar direcciones de lista blanca y negra para cada uno de los módulos de seguridad que propone.	**cumple**
4,13	La solución debe disponer de funciones de validación y autentificación del remitente de manera automática que incluyan:	**cumple**
	- DKIM	**cumple**
	- DMARK	**cumple**
	- SPF	**cumple**

Emilio Peralta
Ministerio de la Defensa Pública

Abg. Ramiro Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Peralta
Ministerio de la Defensa Pública

4,14	La solución debe de disponer de modulo anti malware para la detección oportuna de amenazas conocidas, desconocidas y avanzadas en Microsoft Exchange Online, Microsoft OneDrive, Microsoft SharePoint Online y Microsoft Teams bajo tecnologías de:	cumple
	- Firmas,	cumple
	- Análisis heurísticos	cumple
		cumple
	- Comportamiento.	cumple
4,15	La solucion debe de disponer una visibilidad unificada de las amenazas detectadas por los sevicios de seguridad base de Microsoft Exchange Online mediante la visualizacion de una cuarentena unica.	cumple
4,16	Debe contar con cuadros de mandos, KPIs y reportes de seguimientos de las detecciones realizadas.	cumple
4,17	La solución no debe almacenar datos sensibles como usuarios y contraseñas y para esto debe de poder integrase con Microsoft Office 365 mediante OAuth 2.0	cumple
4,18	La protección de anti-malware para Microsoft SharePoint Online debe permitir la exclusión y selección de sitios protegidos.	cumple
4,19	La protección de anti-malware para Microsoft OneDrive debe permitir la exclusión y selección de usuarios protegidos.	cumple
4,20	Debe contar con protección frente a virus, troyanos y otras clases de malware para MS Teams.	cumple
4,21	Debe disponer de un módulo de supervisión de fuga de datos con el objetivo del descubrimiento de información confidencial transmitida y almacenada por los usuarios en los buzones de correo de Exchange Online, en los almacenamientos de OneDrive y en los sitios de SharePoint Online de la organización relacionadas con datos de tarjetas de crédito.	cumple
4,22	La solución debe contar con capacidades de escaneo retrospectivo de amenazas que incluya los buzones de correo y de Ms Office 365 y los repositorios de datos de OneDrive.	cumple
4,23	Debe contar con protección basada en firmas mediante aprendizaje automático junto con análisis conductuales y heurísticos avanzados.	cumple
4,24	Debe usar una combinación de SPF (marco de directivas de remitente), DKIM (DomainKeys Identified Mail), validación de correo electrónico de DMARC (Autenticación de mensajes, informes y conformidad basada en dominios) y el método de detección de similitudes para detectar y prevenir spoofing y phishing de correos electrónicos, ataques BEC y spam.	cumple
4,25	Debe proveer heurística mediante redes neurales de aprendizaje profundo.	cumple

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Peralta
Ministerio de la Defensa Pública

4,26	Debe incluir protección contra ataques de inyección de código y mailsploit/spoofing que son posibles debido a los errores de los clientes de correo.	**cumple**
4,27	Debe contar con mecanismo de detección de spam al nivel de la dirección IP.	**cumple**
4,28	Debe poder rastrear el intercambio de datos confidenciales de texto o imágenes que se almacenan y transmiten dentro y fuera de su organización, por lo que puede considerar acciones para impedir posibles fugas.	**cumple**
5	**Plataforma Anti-Spam Correo Electrónico**	**cumple**
5,1	La solución debe ser proporcionada mediante Imagen de Software en formato ISO para el despliegue sobre plataforma virtualizada acorde a modalidad gateway virtual.	**cumple**
5,2	La solución debe disponer capacidades de integración con plataforma XDR con el objetivo de proporcionar capacidades avanzadas de detección de amenazas que incluyan la utilización de reglas Yara y procesamiento de correos acorde a módulo de Sandbox on- premise.	**cumple**
5,3	La solución debe ser implementada on-premise y debe disponer de una consola Web de gestión centralizada.	**cumple**
5,4	Los módulos y/o componentes de la solución deben estar basados en software/appliance de uso específico, con sistema operativo, base de datos y servicios configurados para óptimo rendimiento y securitización por el fabricante de la solución.	**cumple**
5,5	La solución debe proveer un procedimiento por el cual se pueda realizar una actualización de todos y cada uno de los dispositivos que la componen, sin la necesidad de realizar un corte de servicio y sin afectar al resto de los componentes	**cumple**
5,6	La solución debe inspeccionar en tiempo real el tráfico de correo (Entrada & Salida) para la remoción de todo tipo de amenazas, virus, worms, troyanos y otros tipos de programas maliciosos incluyendo correos indeseados	**cumple**
5,7	La solución debe de contar con tecnologías de detección Anti-Spam, Anti-Phishing, Anti- Malware, Anti-Ransomware y de filtrado de contenido.	**cumple**
5,8	La solución tiene la capacidad de integración con servicios de reputación locales sin la necesidad de enviar datos fuera de la organización.	**cumple**
5,9	La solución dispone de capacidades para el desempaquetado y análisis de archivos compuestos como por ejemplo archivos comprimidos.	**cumple**
5,10	La solución debe de detectar, bloquear y desinfectar mensajes de correos electrónicos infectados, así como sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.	**cumple**

Emilio Peralta
Ministerio de la Defensa Pública

Lic. Nilda Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Peralta
Ministerio de la Defensa Pública

5,11	La solución debe detectar y bloquear mensajes que contengan anexos con macros (Por ejemplo, archivos en formato Microsoft Office con macros), eliminar mensajes o sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.	cumple
5,12	La solución debe detectar y bloquear mensajes cifrados, eliminar mensajes o sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.	cumple
5,13	La solución debe disponer de capacidad de filtrado de contenido de los mensajes mínimamente acorde al nombre, tamaño y tipo de anexo, determinando el formato indiferentemente de su extensión, así como eliminar mensajes o sus anexos con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.	cumple
5,14	Los mensajes que se encuentran en el backup deben poder ser guardados y descargados, así como reenviados a su destinatario original u otros destinatarios a ser seleccionados.	cumple
5,15	La solución debe de procesar los mensajes, acorde a las reglas de seguridad estipuladas para los grupos de remitentes y destinatarios.	cumple
5,16	La solución debe poder validar el remitente acorde a la autentificación del remitente utilizando tecnologías SPF, DKIM y DMARC.	cumple
5,17	La solución debe poder firmar correos salientes mediante tecnologías DKIM.	cumple
5,18	La solución debe permitir la inclusión de un mensaje de alerta en el subject del correo en caso que anexos peligrosos o indeseados sean detectados.	cumple
5,19	La solución debe permitir la definición de listas de correo blancas/negras globales y personales.	cumple
5,20	La solución debe contar con tecnologías de validación de imágenes y anexos gráficos para la detección de mensajes de Spam.	cumple
5,21	La solución debe identificar archivos sospechosos, potencialmente peligrosos, protegidos con contraseña, así como objetos que han tenido algún error en su análisis. Los mismos deben ser adicionalmente enviados al módulo de Sandbox para su procesamiento.	cumple
5,22	La solución debe poder eliminar mensajes o sus anexos para archivos sospechosos, potencialmente peligrosos, protegidos con contraseña, así como objetos que han tenido algún error en su análisis con la posibilidad de generar una copia de los mismos al ser almacenada en un Backup.	cumple
5,23	La solución debe proporcionar capacidades de detección y protección ante ataques del tipo Business Email Compromise (BEC).	cumple
5,24	La solución debe disponer de tecnologías para la detección de Spam basado en el reconocimiento de dominios spoofed (look-alike).	cumple
5,25	La solución debe de contar con tecnologías proactivas para la detección de amenazas avanzadas o de día 0.	cumple

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

5,26	La solución debe de contar con tecnologías de detección avanzadas para la detección y neutralización de amenazas del tipo ransomware.	**cumple**
5,27	En caso de objetos infectados la solución debe poder configurar la realización de las siguientes acciones:	**cumple**
5,28	Desinfectar	**cumple**
5,29	Eliminar Anexo	**cumple**
5,30	Borrar mensaje	**cumple**
5,31	Rechazar mensaje	**cumple**
5,32	Ignorar	**cumple**
5,33	La solución permite la configuración de notificaciones por lo menos a las siguientes direcciones (Administradores, Remitente, Destinatario, adicionales).	**cumple**
5,34	La solución debe contar con un sistema de alimentación de contenido por parte del fabricante que proporcione información sobre nuevas amenazas, y bases de reputación. Dicha información debe ser actualizada en forma automática y en tiempo real permitiendo enriquecer el motor de análisis de amenazas de la solución.	**cumple**
5,35	La totalidad del análisis y operación de la solución debe realizarse en forma local, solo permitiéndose el envío de hashes cuando sea necesario. La solución no debe enviar ninguna otra información sensible fuera de la institución.	**cumple**
5,36	La solución debe disponer soporte para la integración con Microsoft Active Directory y Open LDAP.	**cumple**
5,37	La solución incluye el acceso al Backup personal mediante Single Sign-On (SSO) acorde a integración con directorio LDAP.	**cumple**
5,38	La solución permite la utilización de expresiones regulares para la composición de reglas de filtrado.	**cumple**
5,39	La consola de administración Web, proporciona capacidades de acceso basado en roles y perfiles de usuario. Role Based Access Control (RBAC).	**cumple**
5,40	La solución cuenta con capacidades para en envió de eventos a un sistema (SIEM) utilizando protocolo Syslog.	**cumple**
5,41	La solución permite la generación de reportes y cuadros de mando acorde al periodo seleccionado (día, semana, mes, año) en formato PDF.	**cumple**

Emilio Peralta
Ministerio de la Defensa Pública

Atilio J. Gómez Ayala
Depto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silpia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Peralta
Ministerio de la Defensa Pública

5,42	La solución debe proporcionar un cuadro de mando web que incluye como mínimo información de: Estado de la Salud del Sistema, Mensajes Procesados (Entrada/Salida) & Amenazas Detectadas.	**cumple**
5,43	La consola Web permite la personalización del cuadro de mando el cual permite configurar múltiples widgets a criterio del administrador de la solución.	**cumple**
5,44	La solución debe poder gestionar múltiples dominios de correo electrónico.	**cumple**
5,45	La solución debe permitir generar reportes en forma manual o programados a intervalos de tiempo determinados.	**cumple**

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Directora
Dirección Jurídica
Ministerio de la Defensa Pública

ASPECTOS GENERALES

1. El proveedor deberá presentar autorización del fabricante, y en caso de representante o distribuidor deberán demostrar que los mismos están autorizados como tal por el Fabricante.	**cumple / presento certificado**
2. El fabricante de las soluciones ofertadas debe brindar soporte a través de una página web, email y línea telefónica.	**cumple**
3. El fabricante de las soluciones ofertadas debe contar con por lo menos 25 años de presencia en el mercado global.	**cumple**
5. 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**

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública

Emilio Perali
Ministerio de Defensa Pública

Capacidad Técnica

El oferente deberá proporcionar evidencia documentada que demuestre su cumplimiento con los siguientes requisitos de capacidad técnica:

1. Contar como mínimo con 1 ingeniero certificado con las certificaciones avanzadas del producto.	**cumple / presento certificado**
2. Contar como mínimo con 1 técnico con certificaciones de cifrado.	**cumple / presento certificado**
3. Contar con por lo menos 1 técnico con certificaciones en protección de servidores de correo antispam	**cumple / presento certificado**
4. El proveedor 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 / presento certificado**
5. El proveedor deberá ser Canal Platinum de la Marca ofertada, para garantizar el buen servicio y respaldo del soporte local, para ello deberá presentar el certificado que lo	**cumple / presento certificado**

Abg. Atilio J. Gómez Ayala
Dpto. de Presupuesto
Ministerio de la Defensa Pública

Abg. Silvia B. Bogado
Directora
Dirección Jurídica
Ministerio de la Defensa Pública