COMITÉ DE EVALUACIÓN – INFORME DE EVALUACIÓN

INFORME DE EVALUACIÓN		
NOMBRE DEL PROCESO	TIPO Y N°	ID
"ADQUISICIÓN DE RENOVACIÓN Y ACTUALIZACIÓN DE SOFTWARE DE SEGURIDAD, CONTROL DE PUNTO FINAL, DETECCIÓN Y RESPUESTA ANTE INCIDENTES Y PROTECCIÓN DE CORREO ELECTRÓNICO PARA EL MSPYBS- AD REFERENDUM"- PLURIANUAL	*LPN SBE Nº 36/23*	*422.466*
INTEGRANTES DEL COMITÉ DE EVALUACIÓN	LUGAR	FECHA Y HORA
• Abg. Vicente Pérez, Representante de la Dirección General de Administración y Finanzas, designado según providencia del Memorándum DLIC-DOC N° 071/2023 de fecha 27/01/2023. • Lic. Leticia Segovia, representante de la Dirección Financiera, designada según providencia del Memorándum DLIC-DOC N° 072/2023 de fecha 27/01/2023. • Ing. Emidal González, Representante de la Dirección General de Tecnologías de la Información y Comunicación, designado según providencia del Memorándum DLIC-DOC N° 073/2023 de fecha 27/01/2023.	Asunción, Paraguay	06/02/2023 – 15:30 Hs.

1. ANTECEDENTES

Resolución D.G.A.F. Nº 3018 de fecha 27/12/2022 *"POR LA CUAL SE AUTORIZA EL LLAMADO, SE APRUEBA EL PLIEGO DE BASES Y CONDICIONES Y SE CONSTITUYE EL COMITÉ DE EVALUACIÓN DE OFERTAS DEL LLAMADO A LICITACIÓN PÚBLICA NACIONAL N° 36/2023 "ADQUISICIÓN DE RENOVACIÓN Y ACTUALIZACIÓN DE SOFTWARE DE SEGURIDAD, CONTROL DE PUNTO FINAL, DETECCIÓN Y RESPUESTA ANTE INCIDENTES Y PROTECCIÓN DE CORREO ELECTRÓNICO PARA EL MSPYBS- AD REFERENDUM"- PLURIANUAL – ID N° 422.466.*

Nota D.G.T.I.C. N° 284/2022 de la Dirección General de Tecnologías de la Información y Comunicación, por la cual se remite el pedido con las especificaciones técnicas y solicita el inicio del proceso de compra.

Dictamen DOC N° 375/22 del 10/12/2022 *"POR EL CUAL SE DETALLA LA METODOLOGÍA UTILIZADA PARA LA OBTENCIÓN DE LOS PRECIOS REFERENCIALES".*

Antes de iniciar la evaluación de ofertas, todos los miembros firman la Declaración Jurada, donde manifiestan no tener conflicto de intereses, con la empresa oferente del presente proceso de contratación.

2. DISPONIBILDAD PRESUPUESTARIA

Que, este proceso cuenta con Disponibilidad Presupuestaria para una eventual adjudicación.

3. ACTA DE APERTURA DE SOBRES

En fecha 26/01/23, se emite el Acta de Sesión Pública Virtual, resultante del proceso de Subasta a la Baja Electrónica, observándose un total de 01 (UN) participante. De acuerdo a lo previsto en el Artículo 57 del Decreto Reglamentario No. 2992/2019, se llevó a cabo el acto de Apertura de Sobres Físicos en fecha 27/01/23 a las 09:15 horas, en el Departamento de Licitaciones – DOC – Nivel Central, observándose la recepción de la oferta del participante del proceso de Subasta a la Baja Electrónica, que se detalla a continuación:

OFERENTE	MONTO TOTAL DE OFERTA
1. Corporation Sekiura S.A.C.E.I - RUC: 80070889-0	Gs. 2.635.000.000

OBSERVACIONES ASENTADAS EN EL ACTA DE APERTURA: ninguna.

4. VERIFICACIÓN DE LA DOCUMENTACIÓN SUSTANCIAL

Conforme a los requisitos de calificación dispuestos en el Artículo 61° del Decreto N° 2992/2019, se verificaron los documentos de carácter sustancial que componen las ofertas presentadas. Se estableció que, a los efectos de indicar su cumplimiento se utilizará el criterio de CUMPLE o NO CUMPLE. *Las siguientes documentaciones fueron objeto de verificación por la representación legal del Comité Evaluador, conforme al ámbito de su competencia.*

N° de Orden	Empresa	Formulario Oferta y Planilla de Precios	Garantía de Mantenimiento de Oferta	Documentos que acrediten las facultades del firmante	Documentos que acrediten la existencia del oferente
1	Corporation Sekiura S.A.C.E.I.	CUMPLE	CUMPLE	CUMPLE	CUMPLE

Abg. Vicente Pérez
Abogado Dictaminante
AJ - DGAF - M.S.P. y B.S.

Lic. Leticia Segovia
D.C.P.P. - D. Financiera
M.S.P. y B.S

Ing. Emidal González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

5. CALIFICACIÓN LEGAL DEL OFERENTE CON RESPECTO A LA PROHIBICIONES PREVISTAS EN EL ARTICULO 40° DE LA LEY Nº 2051/03 "DE CONTRATACIONES PÚBLICAS

Para determinar que la empresa participante no se encuentra comprendida en las prohibiciones establecidas en el Art 40 Inc. a) y b) de la Ley 2051/03, este Comité verificó en el PORTAL ÚNICO DE GOBIERNO (www.paraguay.gov.py) si las personas citadas más abajo, Representantes de la firma oferente, figuran en la base de datos como funcionarios públicos. Los resultados arrojados se detallan en el siguiente cuadro y las constancias de los mismos forman parte del expediente administrativo.

N°	Corporation Sekiura S.A.C.E.I	CI N°	CONSTANCIA N°	OBSERVACIÓN
1	NELIDA RAFAELA APONTE DE FISCHER	397359	4138928	NO REGISTRAN DATOS ACTUALES
2	INGRID FISCHER APONTE	4204194	4138935	

La información proveniente del Sistema de Intercambio de Información entre Instituciones Públicas del Estado al cual se accede a través de la página MITIC, autorizado y reglamentado por Decreto N° 10517/2013, lo cual garantiza que son datos íntegros, confiables y verificables emitidos por cada una de las instituciones.

Que, conforme Memorándum DLIC Nº 069/2023 de fecha 27/01/2023, se solicita a la Dirección General de Asesoría Jurídica, informe sobre rescisión Contractual de la empresa participante, con respecto al cumplimiento de lo dispuesto en el Artículo 40 inciso "c" de la Ley 2051/03.

Que, mediante Memorándum A.J. Nº 36/2023, de fecha 27/01/2023, la Dirección General de Asesoría Jurídica informa cuanto sigue: *"que verificados los registros del Departamento de Archivo/Estadísticas dependiente de la Dirección a mi cargo, no obra antecedentes ni Resoluciones de RESCISIÓN DE CONTRATO CONTRACTUAL con la empresa Corporation Sekiura S.A.C.E.I RUC N° 80070889-0, a partir del ejercicio fiscal 2021 hasta la fecha."*

Así también, según Memorándum D.E.C. N° 51/2023 de fecha 31/01/2023, el Departamento de Ejecución de Contratos - DGAF, informa en contestación al pedido de verificación del cumplimiento del Art. 40 inc. e) requerido por Memorando DLIC Nº 070/2023 del 27/01/2023 cuanto sigue: *"Según los registros del Sistema y los expedientes pendientes de cancelación de la Institución, obrante en esta dependencia no se registran expedientes por incumplimiento contractual."*

Se ha verificado en el SICP el cumplimiento de los incisos m) y n) de la empresa participante, donde el oferente ni aquellos sujetos mencionados en estos incisos; han sido sancionados por la DNCP, conforme a lo previsto en el Art. 72 de la Ley N° 6716/21.

Este Comité de Evaluación, con respaldo documental de los análisis realizados, *determina que la empresa participante no se encuentra comprendida en las prohibiciones establecidas en el Art 40 de la Ley 2051/03.*

6. REGISTRO DE EMPRESAS INHABILITADAS

Se verifica en el Registro de Empresas Inhabilitadas del Portal de la Dirección Nacional de Contrataciones Públicas que el oferente se encuentra habilitado para Contratar con el Estado Paraguayo.

7. SOLICITUDES DE DOCUMENTOS Y ACLARACIÓN DE LAS OFERTAS

Este comité no consideró pertinente realizar consultas al oferente.

8. TABLA COMPARATIVA DE PRECIOS DE LAS OFERTAS

Se realiza el Cuadro Comparativo de Ofertas, teniendo en cuenta el sistema de adjudicación, el cual forma parte íntegra del presente Informe de Evaluación, de acuerdo al ANEXO I. Además, se aplicarán las disposiciones establecidas en el artículo 67 del Decreto Reglamentario N° 2992/2019 de la Ley N° 2051/03 y demás Criterios establecidos en las bases y condiciones del llamado. No fueron requeridas correcciones aritméticas.

9. VERIFICACIÓN DE LOS PRECIOS OFERTADOS POR LAS FIRMAS PARTICIPANTES

Verificado el Cuadro Comparativo de Ofertas, todos los precios cotizados por la firma oferente se ajustan a los rangos permitidos por la DNCP.

Lic. Leticia Segovia
D.C.P.P. - D. Financiera
M.S.P. y B.S.

Abg. Vicente Pérez
Abogado Dictaminante
AJ - DGAF - M.S.P. y B.S.

Ing. Emidal Gonzalez Aguilera
Director
Dirección de Seguridad Informática
DCTIC - MSP y BS

10. CRITERIOS DE MARGEN DE PREFERENCIA Y DESEMPATE DE OFERTAS

Verificación conforme al Pliego de Bases y Condiciones y disposiciones legales vigentes.

MARGEN DE PREFERENCIA PARA PRODUCTOS NACIONALES: atendiendo a que solo se presenta una oferta, este criterio NO APLICA.

MARGEN DE PREFERENCIA LOCAL (MPL): para el asentamiento de esta convocante, el criterio NO APLICA.

CRITERIO PARA DESEMPATE DE OFERTAS: atendiendo a que solo se presenta una oferta, este criterio NO APLICA.

11. VERIFICACIÓN DE LOS DOCUMENTOS LEGALES REQUERIDOS

Que de conformidad al Pliego de Bases y Condiciones, se procede a la evaluación de las Documentaciones Legales y Exigencias, en cumplimiento del Decreto 2992/19 que reglamenta la Ley 2051/03 de Contrataciones Públicas. Asimismo, se estableció que a los efectos de su cumplimiento se utilizará el criterio de ***CUMPLE o NO CUMPLE***, para la CONFORMIDAD DE LA OFERTA EVALUADA CON EL PLIEGO DE BASES Y CONDICIONES, *las cuales fueron objeto de verificación por la representación legal del Comité Evaluador, conforme al ámbito de su competencia y* se exponen en el siguiente cuadro:

REF.	EMPRESA	CONSTANCIA SIPE N°
1	Corporation Sekiura S.A.C.E.I.	1730178

CRITERIO	ABREVIATURA
Cumple	C
No cumple	NC
No presenta	NP
No Aplica	N/A

DOCUMENTOS QUE COMPONEN LA OFERTA	Corporation Sekiura S.A.C.E.I.
1. Formulario de Oferta (*)	C FS. 1-3
2. Garantía de Mantenimiento de Oferta (*)	C FS. 7-9
3. Certificado de Cumplimiento con la Seguridad Social (**)	C SIPE
4. Certificado de Producto y Empleo Nacional, emitido por el MIC, en caso de contar. (**)	N/A
5. Constancia de presentación de la "Declaración Jurada de bienes y rentas, activos y pasivos" ante la Contraloría General de la República, para los sujetos obligados en el marco de la Ley N° 6355/19. (**)	N/A
6. Declaración Jurada de Declaración Jurada de Miembros, de conformidad con el formulario estándar Sección Formularios (**)	C FS. 17
7. Certificado de Cumplimiento Tributario. (**)	C SIPE
8. Patente comercial del municipio en donde esté asentado el establecimiento principal del oferente. (**)	C FS. 12
9. Documentos legales	
9.1 Oferentes Individuales. Personas Físicas.	N/A
9.2 Oferentes Individuales. Personas Jurídicas.	
Fotocopia simple de los documentos que acrediten la existencia legal de la persona jurídica tales como la Escritura Pública de Constitución y protocolización de los Estatutos Sociales. Los estatutos deberán estar inscriptos en la Sección Personas Jurídicas de la Dirección de Registros Públicos. (*)	C SIPE
Constancia de inscripción en el Registro Único de Contribuyentes y fotocopia simple de los documentos de identidad de los representantes o apoderados de la sociedad.	C SIPE
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. (*)	C SIPE
9.3 Oferentes en Consorcio.	N/A

12. ANÁLISIS DE CAPACIDAD FINANCIERA

Se verifica el cumplimiento de los Requisitos documentales para este criterio:

DOCUMENTOS QUE COMPONEN LA OFERTA	Corporation Sekiura S.A.C.E.I
Balance General y Estado de Resultados de los años 2019, 2020, 2021 para contribuyente de IRACIS/IRE GENERAL	C SIPE
Presentación del Formulario N° 106, año 2019, y 501 años 2020 y 2021 para los contribuyentes IRPC/IRE/IRE SIMPLE.	N/A
Presentación del Formulario N° 104 año 2019 y 515 años 2020 y 2021 para los contribuyentes del IRP/IRP-RSP.	N/A
Para contribuyentes de IVA Formularios IVA General: de los 6 seis últimos meses.	N/A

Lic. Leticia Segovia
M.C.P.P. - D. Financiera
M.S.P. y B.S.

Ing. Emidal González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

Abg. Vicente Pérez
Abogado Dictaminante
AJ - DGAF - M.S.P. y B.S.

COMITÉ DE EVALUACIÓN – INFORME DE EVALUACIÓN

El Comité de Evaluación ha realizado del ANÁLISIS DE RATIOS FINANCIEROS de la Empresa Oferente, a fin de determinar si la misma cuenta con las calificaciones y la capacidad financiera necesaria para ejecutar contratos.

EMPRESA	ÍNDICE	PROMEDIO	CALIFICACIÓN
Corporation Sekiura S.A.C.E.I.	RATIO DE LIQUIDEZ	1,61	CUMPLE
	ENDEUDAMIENTO	0,42	
	RENTABILIDAD	0,45	

Los cálculos realizados a fin de llegar a los resultados del cuadro anterior, se encuentran detallados en el ANEXO II al presente Informe de Evaluación.

13. ANÁLISIS DE EXPERIENCIA REQUERIDA

Se verifica el cumplimiento de los Requisitos documentales para este criterio:

REQUISITOS DOCUMENTALES	Corporation Sekiura S.A.C.E.I.
Copias de Contratos, facturas y/o recepciones finales que avalen la experiencia requerida de bienes similares de los Ejercicios Fiscales 2019 2020 y 2021.	C FS. 93-149

ÍNDICE 1: Demostrar experiencia en la provisión de Implementación de Licencias Antivirus, con copias de contratos ejecutados, facturaciones de venta y/o recepciones finales por un monto equivalente al 30 % como mínimo del monto total ofertado en la presente licitación, de los últimos 3 (tres) años (2019 - 2020 y 2021). Para este punto se deberá presentar Copias de Contratos, facturas y/o recepciones finales que avalen la experiencia requerida de bienes similares de los Ejercicios Fiscales 2019 2020 y 2021.

EMPRESA	MONTO TOTAL OFERTADO	30 % COMO MINIMO DEL MONTO TOTAL OFERTADO	EXPERIENCIA CON CONTRATOS EJECUTADOS y FACTURACIONES	INDICE 1
Corporation Sekiura S.A.C.E.I.	2.635.000.000	790.500.000	1.583.450.000	CUMPLE

14. VERIFICACIÓN DE LA CAPACIDAD TÉCNICA Y CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS

Que, de conformidad al Pliego de Bases y Condiciones, se procede a la evaluación de las Documentaciones Técnicas, en cumplimiento del Decreto 2992/19 que reglamenta la Ley 2051/03 de Contrataciones Públicas. Asimismo, se estableció que a los efectos de su cumplimiento se utilizará el criterio de *CUMPLE o NO CUMPLE*, para la CONFORMIDAD DE LA OFERTA EVALUADA CON LAS BASES Y CONDICIONES, *las cuales fueron objeto de verificación por la representación Técnica del Comité Evaluador, conforme al ámbito de su competencia. En virtud del Art 63° del Decreto N° 2992/19* se expone en el siguiente cuadro el resultado de análisis de la oferta presentada:

Ítem	Descripción	Corporation Sekiura S.A.C.E.I.	
		Capacidad Técnica	EETT
1	Antivirus Corporativo con antispyware y antispam	CUMPLE	CUMPLE
2	Servicio técnico / soporte para equipos informáticos	CUMPLE	CUMPLE

Conforme a las Bases y Condiciones del llamado se procedió a verificar el cumplimiento de las capacidades técnicas, especificaciones técnicas y muestras presentadas. El detalle de la evaluación se encuentra detallado en el ANEXO III.

15. RECOMENDACIONES DE LA COMISIÓN EVALUADORA

En base a las consideraciones expuestas en el presente informe y de conformidad a los Artículos 26, 27 y 28 de la Ley N° 2051/03 "De Contrataciones Públicas" y los Artículos 59 al 63 del Decreto Reglamentario N° 2992/19, *el Comité de Evaluación de Ofertas, Sugiere y Recomienda*:

a) ADJUDICAR la presente licitación, en virtud a que la empresa oferente cumple con los requerimientos económicos, técnicos y con las especificaciones técnicas solicitadas; conforme al siguiente detalle:

Abg. Vicente Pérez
Abogado Dictaminante
AJ - DGAF - M.S.P. y B.S.

Lic. Leticia Segovia
D.C.P.P. - D. Financiera
M.S.P. y B.S.

Ing. Emidal Gonzalez Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

Corporation Sekiura S.A.C.E.I.

Ítem	Código Catálogo	Descripción del Bien	Unidad de Medida	Presentación	Cantidad	Marca	Procedencia	Precio unitario (IVA incluido)	Precio total
1	43233205-002	Antivirus Corporativo con antispyware y antispam	Unidad	Unidad	2.000	Kaspersky	Reino Unido	717.500	1.435.000.000
2	81111811-001	Servicio técnico / soporte para equipos informáticos	Unidad	Unidad	1	Sekiura	Paraguay	1.200.000.000	1.200.000.000
Precio Total									2.635.000.000

MONTO TOTAL: GUARANÍES DOS MIL SEISCIENTOS TREINTA Y CINCO MILLONES.-

Con lo que se dio por terminado el acto en fecha 20. de febrero de 2023.

ES NUESTRO INFORME.

Lic. Leticia Segovia
D.C.P.P. - D. Financiera
M.S.P. y B.S.

Ing. Emidal González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

Abg. Vicente Pérez
Abogado Dictaminante
AJ - DGAF - M.S.P. y B.S.

ANEXO I

CUADRO COMPARATIVO DE OFERTAS

CUADRO COMPARATIVO DE OFERTAS

LPN N° 36/2023 ADQUISICIÓN DE RENOVACIÓN Y ACTUALIZACIÓN DE SOFTWARE DE SEGURIDAD, CONTROL DE PUNTO FINAL, DETECCIÓN Y RESPUESTA ANTE INCIDENTES Y PROTECCIÓN DE CORREO ELECTRÓNICO PARA EL MSPYBS- AD REFERENDUM - PLURIANUAL - ID: 422466

							Corporation Sekiura S.A.C.E.I			
Ítem	Código Catálogo	Descripción del Bien	Unidad de Medida	Presentación	Precio Unitario Referencial	Cantidad	Marca	Procedencia	Precio unitario (IVA incluído)	Precio total	% Variación
1	43233205-002	Antivirus Corporativo con antispyware y antispam	Unidad	Unidad	722.583	2.000	Kaspersky	Reino Unido	717.500	1.435.000.000	-1
2	81111811-001	Servicio técnico / soporte para equipos informaticos	Unidad	Unidad	1.204.833.333	1	Sekiura	Paraguay	1.200.000.000	1.200.000.000	-0
									Precio Total	**2.635.000.000**	

Lic. Leticia Segovia
D.C.P.P. - D. Financiera
M.S.P y B.S.

Ing. Emidal Gonzalez Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

Abg. Vicente Pérez
Abogado Dictaminante
AJ - DGAF - M.S.P. y B.S.

ANEXO II

ANÁLISIS FINANCIERO Y EXPERIENCIA REQUERIDA

DIRECCIÓN GENERAL DE ADMINISTRACIÓN Y FINANZAS
COMITÉ DE EVALUACIÓN

INFORME DE EVALUACIÓN FINANCIERA

REF : **REMISIÓN DE ANÁLISIS DE CAPACIDAD FINANCIERA Y EXPERIENCIA REQUERIDA LPN N° 36/2023**

ELABORADO POR: **LIC. MARÍA LETICIA SEGOVIA GÓMEZ,** MIEMBRO
COMITÉ DE EVALUACIÓN LCO LPN N° 36/2023

En el marco de la **LPN N° 36/2023** *"ADQUISICIÓN DE RENOVACIÓN Y ACTUALIZACIÓN DE SOFTWARE DE SEGURIDAD, CONTROL DE PUNTO FINAL, DETECCIÓN Y RESPUESTA ANTE INCIDENTES Y PROTECCIÓN DE CORREO ELECTRÓNICO PARA EL MSPYBS- AD REFERENDUM - PLURIANUAL"*– **ID N° 422466**, remito el informe de ratios financieros sobre las documentaciones presentadas por las firmas oferentes de la mencionada Licitación.

Al respecto remito adjunto los resultados arrojados según datos de las copias de Balances de los años 2019, 2020 2021, respectivamente; y la experiencia requerida en concordancia con lo establecido en el Pliego de Bases y Condiciones.

1. ANÁLISIS DE CAPACIDAD FINANCIERA

Se verifica el cumplimiento de los Requisitos documentales para este criterio:

REQUISITOS DOCUMENTALES	REQUISITO
Balance General y Estado de Resultados de los años 2019, 2020, 2021 para contribuyente de IRACIS/IRE GENERAL.	R1
Presentación del Formulario N° 106, año 2019, y 501 año 2020 y 2021 para los contribuyentes IRPC/IRE/IRE SIMPLE.	R2
Presentación del Formulario N° 104 año 2019 y 515 años 2020 y 2021 para los contribuyentes del IRP/IRP-RSP.-.	R3
Para contribuyentes Formularios IVA General: de los 6 seis últimos meses	R4

	OFERENTES	R1	R2	R3	R4
1	**Corporation Sekiura S.A.C.E.I.**	Cumple SIPE Fs. 10-11	N/A	N/A	N/A

El Comité de Evaluación procede a la elaboración del ANÁLISIS DE RATIOS FINANCIEROS de las Empresas Oferentes, a fin de determinar si las mismas cuentan con las calificaciones y la capacidad financiera necesaria para ejecutar contratos.

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

INDICES FINANCIEROS		AÑO 2019		AÑO 2020		AÑO 2021		PROMEDIO	CALIFICACION
		MONTO G.	ÍNDICE	MONTO G.	ÍNDICE	MONTO G.	ÍNDICE		
RATIO DE LIQUIDEZ	ACTIVO CORRIENTE / PASIVO CORRIENTE	2.890.205.938 / 1.788.612.648	1,62	3.268.169.128 / 1.847.225.761	1,77	3.658.505.966 / 2.521.355.843	1,45	1,61	CUMPLE
ENDEUDAMIENTO	PASIVO TOTAL / ACTIVO TOTAL	1.788.612.648 / 3.866.642.840	0,46	1.847.225.761 / 4.646.424.691	0,40	2.521.355.843 / 6.198.999.052	0,41	0,42	CUMPLE
RENTABILIDAD	UTILIDAD D/ IMPUESTOS / CAPITAL	313.364.717 / 1.000.000.000	0,31	685.110.301 / 1.000.000.000	0,69	878.444.279 / 2.600.000.000	0,34	0,45	CUMPLE

Lic. Leticia Segovia
D.G.P.P. - D. Financiera
M.S.P. y B.S.

2. ANÁLISIS DE EXPERIENCIA REQUERIDA

Se verifica el cumplimiento de los Requisitos documentales para este criterio:

ÍNDICE: Demostrar experiencia en la provisión de Implementación de Licencias Antivirus, con copias de contratos ejecutados, facturaciones de venta y/o recepciones finales por un monto equivalente al 30 % como mínimo del monto total ofertado en la presente licitación, de los últimos 3 (tres) años (2019 - 2020 y 2021). Para este punto se deberá presentar Copias de Contratos, facturas y/o recepciones finales que avalen la experiencia requerida de bienes similares de los Ejercicios Fiscales 2019 2020 y 2021.-

REQUISITOS DOCUMENTALES	REQUISITO
Copias de Contratos, facturas y/o recepciones finales que avalen la experiencia requerida de bienes similares de los Ejercicios Fiscales 2019 2020 y 2021	R1

OFERENTE	EMPRESAS	R1
1	**Corporation Sekiura S.A.C.E.I.**	Cumple Fs. 66-76

Conforme a la cantidad de Contratos/facturas presentadas por la firma **Corporation Sekiura S.A.C.E.I.**, se deja constancia que han sido analizadas parcialmente, hasta cubrir el monto, del monto mínimo requerido.

EMPRESA	MONTO TOTAL OFERTADO	30 % COMO MINIMO DEL MONTO TOTAL OFERTADO	EXPERIENCIA CON CONTRATOS EJECUTADOS y FACTURACIONES	Experiencia demostrada con contratos/ facturas
Corporation Sekiura S.A.C.E.I.	2.635.000.000	**790.500.000**	1.583.450.000	**CUMPLE**

Se remite el informe, para los fines pertinentes.

Atentamente.

Lic. Leticia Segovia
D.C.P.P. - D. Financiera
M.S.P. y B.S.

ANEXO III

ANÁLISIS CAPACIDAD TÉCNICA – EETT

INFORME DE EVALUACIÓN TÉCNICA

LPN 36/2023 ADQUISICIÓN DE RENOVACIÓN Y ACTUALIZACIÓN DE SOFTWARE DE SEGURIDAD, CONTROL DE PUNTO FINAL, DETECCIÓN Y RESPUESTA ANTE INCIDENTES Y PROTECCIÓN DE CORREO ELECTRÓNICO PARA EL MSPYBS- AD REFERENDUM"- PLURIANUAL

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
Marca	Kaspersky	CUMPLE
Cantidad	2000 (dos mil)	CUMPLE
Vigencia	El proveedor deberá entregar licencias con vigencia de 36 meses.	CUMPLE
1. Servidor de Administración y Consola Administrativa	1. Compatibilidad: 1. Microsoft Windows 10 20H2 32 bits o 64 bits (versiones 12.2 en adelante). 2. Microsoft Windows 10 20H1 32 bits o 64 bits (versiones 12.1 en adelante). 3. Microsoft Windows 10 Enterprise 2019 LTSC 32 bits / 64 bits. 4. Microsoft Windows 10 Enterprise 2016 LTSB 32 bits / 64 bits. 5. Microsoft Windows 10 Enterprise 2015 LTSB 32 bits / 64 bits. 6. Microsoft Windows 10 Pro RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits. 7. Microsoft Windows 10 Pro para estaciones de trabajo RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits. 8. Microsoft Windows 10 Enterprise RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits. 9. Microsoft Windows 10 Education RS5 (actualización de octubre de 2018, 1809) de 32 bits o 64 bits. 10. Microsoft Windows 10 Pro 19H1 32 bits / 64 bits. 11. Microsoft Windows 10 Pro for Workstations 19H1 32 bits / 64 bits. 12. Microsoft Windows 10 Enterprise 19H1 32 bits / 64 bits 13. Microsoft Windows 10 Education 19H1 32 bits / 64 bits. 14. Microsoft Windows 10 Pro 19H2 32 bits / 64 bits. 15. Microsoft Windows 10 Pro for Workstations 19H2 32 bits / 64 bits. 16. Microsoft Windows 10 Enterprise 19H2 32 bits / 64 bits. 17. Microsoft Windows 10 Education 19H2 32 bits / 64 bits. 18. Microsoft Windows 8.1 Pro 32 bits / 64 bits. 19. Microsoft Windows 8.1 Enterprise 32 bits / 64 bits. 20. Microsoft Windows 8 Pro 32 bits / 64 bits. 21. Microsoft Windows 8 Enterprise 32 bits / 64 bits. 22. Microsoft Windows 7 Professional con Service Pack 1 y versiones posteriores 32 bits / 64 bits. 23. Microsoft Windows 7 Enterprise / Ultimate con Service Pack 1 y versiones posteriores 32 bits / 64 bits. 24. Windows Server 2019 Standard 64 bits. 25. Windows Server 2019 Core 64 bits. 26. Windows Server 2019 Datacenter 64 bits. 27. Windows Server 2016 Server Standard RS3 (v1709) (LTSB / CBB) 64 bits. 28. Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB / CBB) 64 bits. 29. Windows Server 2016 Server Core RS3 (v1709) 30. Windows Server 2016 Standard (LTSB) 64 bits. 31. Windows Server 2016 Server Core 32. Windows Server 2016 Datacenter (LTSB) 64 bits. 33. Windows Server 2012 R2 Standard 64 bits. 34. Windows Server 2012 R2 Server Core 64 bits. 35. Windows Server 2012 R2 Foundation 64 bits. 36. Windows Server 2012 R2 Essentials 64 bits. 37. Windows Server 2012 R2 Datacenter 64 bits. 38. Windows Server 2012 Standard 64 bits. 39. Windows Server 2012 Server Core 64 bits. 40. Windows Server 2012 Foundation 64 bits. 41. Windows Server 2012 Essentials 64 bits.	CUMPLE

Ing. Emidal Gonzalez Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	42. Windows Server 2012 Datacenter 64 bits. 43. Windows Storage Server 2016 64 bits. 44. Windows Storage Server 2012 R2 64 bits. 45. Windows Storage Server 2012 64 bit	
2. Características	2.1.1. Se debe acceder a la consola vía WEB (HTTPS) o MMC; 2.1.2. Compatibilidad con Windows FailoverClustering u otra solución de alta disponibilidad 2.1.3. Capacidad de eliminar remotamente cualquier solución antivirus (propia o de terceros) que esté presente en las estaciones y servidores, sin la necesidad de la contraseña de remoción del actual antivirus; 2.1.4. Capacidad de instalar remotamente la solución de antivirus en las estaciones y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory; 2.1.5. Capacidad de instalar remotamente la solución de seguridad en smartphones y Android, utilizando estaciones como intermediadoras; 2.1.6. Capacidad de instalar remotamente la solución de seguridad en smartphones y tablets de sistema iOS; 2.1.7. Capacidad de instalar remotamente cualquier app en smartphones y tablets de sistema iOS; 2.1.8. Capacidad de gestionar estaciones de trabajo y servidores de archivos (tanto Windows como Linux y Mac) protegidos por la solución antivirus; 2.1.9. Capacidad de gestionar smartphones y tablets (tanto Symbian como Windows Mobile, BlackBerry, Android y iOS) protegidos por la solución antivirus; 2.1.10. Capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto; 2.1.11. Capacidad de actualizar los paquetes de instalación con las últimas vacunas, para que cuando el paquete sea utilizado en una instalación ya contenga las últimas vacunas lanzadas; 2.1.12. Capacidad de hacer distribución remota de cualquier software, o sea, debe ser capaz de remotamente enviar cualquier software por la estructura de gerenciamiento de antivirus para que sea instalado en las máquinas clientes; 2.1.13. Capacidad de desinstalar remotamente cualquier software instalado en las máquinas clientes; 2.1.14. Capacidad de aplicar actualizaciones de Windows remotamente en las estaciones y servidores; 2.1.15. Capacidad de importar la estructura de Active Directory para encontrar máquinas; 2.1.16. Capacidad de monitorear diferentes subnets de red con el objetivo de encontrar máquinas nuevas para que sean agregadas a la protección; 2.1.17. Capacidad de monitorear grupos de trabajos ya existentes y cualquier grupo de trabajo que sea creado en la red, a fin de encontrar máquinas nuevas para ser agregadas a la protección; 2.1.18. 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; 2.1.19. Capacidad de agrupamiento de máquinas por características comunes entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antivirus instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 2 días, etc.;	CUMPLE

Ing. Emidal González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	2.1.20. Capacidad de definir políticas de configuraciones diferentes por grupos de estaciones, permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos; 2.1.21. Debe proporcionar las siguientes informaciones de las computadoras: 2.1.21.1. Si el antivirus está instalado; 2.1.21.2. Si el antivirus ha iniciado; 2.1.21.3. Si el antivirus está actualizado; 2.1.21.4. Minutos/horas desde la última conexión de la máquina con el servidor administrativo; 2.1.21.5. Minutos/horas desde la última actualización de vacunas 2.1.21.6. Fecha y horario de la última verificación ejecutada en la máquina; 2.1.21.7. Versión del antivirus instalado en la máquina; 2.1.21.8. Si es necesario reiniciar la computadora para aplicar cambios; 2.1.21.9. Fecha y horario de cuando la máquina fue encendida; 2.1.21.10. Cantidad de virus encontrados (contador) en la máquina; 2.1.21.11. Nombre de la computadora; 2.1.21.12. Dominio o grupo de trabajo de la computadora; 2.1.21.13. Fecha y horario de la última actualización de vacunas; 2.1.21.14. Sistema operativo con Service Pack; 2.1.21.15. Cantidad de procesadores; 2.1.21.16. Cantidad de memoria RAM; 2.1.21.17. Usuario(s) conectados en ese momento, con información de contacto (si están disponibles en el Active Directory) 2.1.21.18. Dirección IP; 2.1.21.19. Aplicativos instalados, inclusive aplicativos de terceros, con historial de instalación, conteniendo fecha y hora que el software fue instalado o removido. 2.1.21.20. Actualizaciones de Windows Updates instaladas 2.1.21.21. Información completa de hardware conteniendo: procesadores, memoria, adaptadores de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD 2.1.21.22. Vulnerabilidades de aplicativos instalados en la máquina 2.1.22. Debe permitir bloquear las configuraciones del antivirus instalado en las estaciones y servidores de manera que el usuario no consiga modificarlas; 2.1.23. Capacidad de reconectar máquinas clientes al servidor administrativo más próximo, basado en reglas de conexión como: 2.1.23.1. Cambio de gateway; 2.1.23.2. Cambio de subnet DNS; 2.1.23.3. Cambio de dominio; 2.1.23.4. Cambio de servidor DHCP; 2.1.23.5. Cambio de servidor DNS; 2.1.23.6. Cambio de servidor WINS; 2.1.23.7. Aparición de nueva subnet; 2.1.24. Capacidad de configurar políticas móviles para que cuando una computadora cliente esté fuera de la estructura de protección pueda actualizarse vía internet; 2.1.25. Capacidad de instalar otros servidores administrativos para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes; 2.1.26. Capacidad de interrelacionar servidores en estructura de jerarquía para obtener informes sobre toda la estructura de antivirus; 2.1.27. Capacidad de herencia de tareas y políticas en la estructura jerárquica de servidores administrativos;	

Ing. Emidal González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	2.1.28. Capacidad de elegir cualquier computadora cliente como repositorio de vacunas y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red; 2.1.29. Capacidad de hacer de este repositorio de vacunas un gateway para conexión con el servidor de administración, para que otras máquinas que no logran conectarse directamente al servidor puedan usar este gateway para recibir y enviar informaciones al servidor administrativo. 2.1.30. Capacidad de exportar informes para los siguientes tipos de archivos: PDF, HTML y XML. 2.1.31. Capacidad de generar traps SNMP para monitoreo de eventos; 2.1.32. Capacidad de enviar correos electrónicos para cuentas específicas en caso de algún evento; 2.1.33. Debe tener compatibilidad con Microsoft NAP, cuando se instale en Windows 2008 Server; 2.1.34. Debe tener documentación de la estructura del banco de datos para generación de informes a partir de herramientas específicas de consulta (CrystalReports, por ejemplo). 2.1.35. Capacidad de conectar máquinas vía Wake on Lan para realización de tareas (barrido, actualización, instalación, etc.), inclusive de máquinas que estén en subnets diferentes del servidor); 2.1.36. Capacidad de habilitar automáticamente una política en caso de que ocurra una epidemia en la red (basado en cantidad de virus encontrados en determinado intervalo de tiempo); 2.1.37. Capacidad de realizar actualización incremental de vacunas en las computadoras clientes; 2.1.38. Capacidad de reportar vulnerabilidades de software presentes en las computadoras. 2.1.39. Capacidad de realizar inventario de hardware de todas las máquinas clientes; 2.1.40. Capacidad de realizar inventario de aplicativos de todas las máquinas clientes; 2.1.41. Capacidad de diferenciar máquinas virtuales de máquinas físicas;	
3. Estaciones Windows	3.1. Compatibilidad: 3.1.1. Windows 10 3.1.2. Windows 8.1 3.1.3. Windows 8 3.1.4. Windows 7 todas las versiones con o sin Service Pack 1 o superior 3.1.5. Windows XP Embedded SP3 (32 bits) 3.1.6. Windows Embedded POSReady 2009 (32 bits) 3.1.7. Windows Embedded Standard 7 SP1 (32 bits, 64 bits) 3.1.8. Windows Embedded Enterprise 7 SP1 (32 bits, 64 bits) 3.1.9. Windows Embedded POSReady 7 (32 bits, 64 bits) 3.1.10. Estándar de Windows Embedded 8.0 (32 bits, 64 bits) 3.1.11. Windows Embedded 8.1 Industry Professional/Empresarial (32 bits, 64 bits) 3.1.12. Windows 10 IoT Enterprise (32 bits, 64 bits) 3.1.13. Windows XP Professional SP2 / SP3 (32 bits) 3.2. Características: 3.2.1. Debe proporcionar las siguientes protecciones: 3.2.1.1. Antivirus de archivos residente (antispyware, antitroyano, antimalware, antiransomware, análisis de comportamiento y detección de anomalías, etc.) que verifique	CUMPLE

Ing. Emidal González Agüero
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	cualquier archivo creado, accedido o modificado; 3.2.1.2. Antivirus de web (módulo para verificación de sitios y downloads contra virus) 3.2.1.3. Antivirus de correo electrónico (módulo para verificación de correos recibidos y enviados, así como sus adjuntos) 3.2.1.4. Antivirus de mensajes instantáneos (módulo para verificación de mensajes instantáneos, como ICQ, MSN, IRC, etc.) 3.2.1.5. Firewall con IDS 3.2.1.6. Autoprotección (contra ataques a los servicios/procesos del antivirus) 3.2.1.7. Control de dispositivos externos 3.2.1.8. Control de acceso a sitios por categoría 3.2.1.9. Control de ejecución de aplicativos 3.2.1.10. Control de vulnerabilidades de Windows y de los aplicativos instalados 3.2.2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota; 3.2.3. Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo). 3.2.4. Capacidad de automáticamente deshabilitar el Firewall de Windows (en caso de que exista) durante la instalación, para evitar incompatibilidad con el Firewall de la solución; 3.2.5. Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación; 3.2.6. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, (ej.: Win32.Trojan.banker) para que cualquier objeto detectado con el resultado elegido sea ignorado; 3.2.7. Capacidad de agregar aplicativos a una lista de aplicativos confiables, donde las actividades de red, actividades de disco y acceso al registro de Windows no serán monitoreadas; 3.2.8. Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks); 3.2.9. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento; 3.2.10. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo; 3.2.11. Capacidad de verificar solamente archivos nuevos y modificados; 3.2.12. Capacidad de verificar objetos usando heurística;	

Ing. Emidal Gonzalez Aguilera
Director
Dirección de Seguridad Informático
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	3.2.13. Capacidad de agendar una pausa en la verificación; 3.2.14. Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo; 3.2.15. El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe: 3.2.15.1. Preguntar qué hacer, o; 3.2.15.2. Bloquear el acceso al objeto; 3.2.15.2.1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador); 3.2.15.2.2. Caso positivo de desinfección: 3.2.15.2.2.1. Recuperar el objeto para uso; 3.2.15.2.3. Caso negativo de desinfección: 3.2.15.2.3.1. Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador); 3.2.16. Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto. 3.2.17. Capacidad de verificar correos electrónicos recibidos y enviados en los protocolos POP3, IMAP, NNTP, SMTP y MAPI, así como conexiones cifradas (SSL) para POP3 y IMAP (SSL); 3.2.18. Capacidad de verificar tráfico de ICQ, MSN, AIM y IRC contra virus y enlaces phishings; 3.2.19. Capacidad de verificar enlaces introducidos en correos electrónicos contra pishings; 3.2.20. Capacidad de verificar tráfico SSL en los browsers: Internet Explorer, Firefox y Opera; 3.2.21. Capacidad de verificación del cuerpo del correo electrónico y adjuntos usando heurística; 3.2.22. El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe: 3.2.22.1. Preguntar qué hacer, o; 3.2.22.2. Bloquear el correo electrónico; 3.2.22.2.1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador); 3.2.22.2.2. Caso positivo de desinfección: 3.2.22.2.2.1. Recuperar el correo electrónico al usuario; 3.2.22.2.3. Caso negativo de desinfección: 3.2.22.2.3.1. Mover a cuarentena o borrar el objeto (de acuerdo con la configuración preestablecida por el administrador); 3.2.23. En caso de que el correo electrónico contenga código que parece ser, pero no es definitivamente malicioso, este debe mantenerse en cuarentena. 3.2.24. Posibilidad de verificar solamente correos electrónicos recibidos, o recibidos y enviados. 3.2.25. Capacidad de filtrar adjuntos de correos electrónicos, borrándolos o renombrándolos de acuerdo con la configuración hecha por el administrador. 3.2.26. Capacidad de verificación de tráfico HTTP y cualquier script de Windows Script Host (JavaScript, Visual Basic Script, etc.) usando heurísticas; 3.2.27. Debe tener soporte total al protocolo IPv6;	

Ing. Emidal González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	3.2.28. Capacidad de modificar las puertas monitoreadas por los módulos de web y correo electrónico; 3.2.29. En la verificación de tráfico web, en caso de que se encuentre código malicioso el programa debe: 3.2.29.1. Preguntar qué hacer, o; 3.2.29.2. Bloquear el acceso al objeto y mostrar un mensaje sobre el bloqueo, o; 3.2.29.3. Permitir acceso al objeto; 3.2.30. El antivirus de web debe realizar la verificación de, como mínimo, dos maneras diferentes, a elección del administrador: 3.2.30.1. Verificación on-the-fly, donde los datos se verifican mientras son recibidos en tiempo real, o; 3.2.30.2. Verificación de buffer, donde los datos se reciben y son almacenados para posterior verificación. 3.2.31. Posibilidad de agregar sitios de la web en una lista de exclusión, donde no serán verificados por el antivirus de web. 3.2.32. Debe contar con módulo que analice las acciones de cada aplicación en ejecución en la computadora, grabando las acciones ejecutadas y comparándolas con secuencias características de actividades peligrosas. Tales registros de secuencias deben ser actualizados conjuntamente con las vacunas. 3.2.33. Debe contar con módulo que analice cada macro de VBA ejecutado, buscando señales de actividad maliciosa. 3.2.34. Debe contar con módulo que analice cualquier intento de edición, exclusión o grabación del registro, de forma que sea posible elegir claves específicas para ser monitoreadas y/o bloqueadas. 3.2.35. Debe tener módulo de bloqueo de Phishing, con actualizaciones incluidas en las vacunas, obtenidas por Anti-PhishingWorkingGroup (http://www.antiphishing.org/). 3.2.36. Capacidad de distinguir diferentes subnets y brindar opción de activar o no el firewall para una subnet específica; 3.2.37. Debe tener módulo IDS (IntrusionDetectionSystem) para protección contra portscans y exploración de vulnerabilidades de software. La base de datos de análisis debe actualizarse conjuntamente con las vacunas. 3.2.38. El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas: 3.2.38.1. Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas; 3.2.38.2. Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de	

Ing. Emidal Gonzalez Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados. 3.2.39. Debe tener módulo que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínimo: 3.2.39.1. Discos de almacenamiento locales 3.2.39.2. Almacenamiento extraíble 3.2.39.3. Impresoras 3.2.39.4. CD/DVD 3.2.39.5. Drives de disquete 3.2.39.6. Modems 3.2.39.7. Dispositivos de cinta 3.2.39.8. Dispositivos multifuncionales 3.2.39.9. Lectores de smart card 3.2.39.10. Dispositivos de sincronización vía ActiveSync (Windows CE, Windows Mobile, etc.) 3.2.39.11. Wi-Fi 3.2.39.12. Adaptadores de red externos 3.2.39.13. Dispositivos MP3 o smartphones 3.2.39.14. Dispositivos Bluetooth 3.2.40. Capacidad de liberar acceso a un dispositivo específico y usuarios específicos por un período de tiempo específico, sin la necesidad de deshabilitar la protección, sin deshabilitar el gerenciamiento central o de intervención local del administrador en la máquina del usuario. 3.2.41. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por usuario. 3.2.42. Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por agendamiento. 3.2.43. Capacidad de configurar nuevos dispositivos por Class ID/Hardware ID 3.2.44. Capacidad de limitar el acceso a sitios de internet por categoría, por contenido (video, audio, etc.), con posibilidad de configuración por usuario o grupos de usuarios y agendamiento. 3.2.45. Capacidad de limitar la ejecución de aplicativos por hash MD5, nombre del archivo, versión del archivo, nombre del aplicativo, versión del aplicativo, fabricante/desarrollador, categoría (ej.: navegadores, gerenciador de download, juegos, aplicación de acceso remoto, etc.). 3.2.46. Capacidad de bloquear la ejecución de un aplicativo que esté en almacenamiento externo. 3.2.47. Capacidad de limitar el acceso de los aplicativos a recursos del sistema, como claves de registro y carpetas/archivos del sistema, por categoría, fabricante o nivel de confianza del aplicativo. 3.2.48. Capacidad de, en caso de epidemia, activar una política alternativa donde cualquier	

Ing. Emidal González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web. 3.2.49. Capacidad de, en caso de que la computadora cliente salga de la red corporativa, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web. 3.2.50. Capacidad de funcionar de forma eficaz incluso con hardware de gama baja (desde 256 MB de RAM y CPU Pentium III) y software antiguo (desde Windows XP) sin riesgo de sobrecargar los sistemas 3.2.51. Supervisión de la integridad del sistema. 3.2.52. Supervisión de la integridad de archivos: Capacidad de realizar el seguimiento de las acciones llevadas a cabo por los archivos y las carpetas especificados dentro de un marco determinado. Además, de poder configurarse que se realice el seguimiento de las modificaciones durante los periodos en los que la supervisión se interrumpe. 3.2.53. Inspección de registros: Capacidad de supervisar las posibles infracciones en relación con la protección mediante la inspección de los registros de eventos de Windows. Posibilidad de que la aplicación envíe una notificación al administrador cuando detecta comportamientos anormales que pueden indicar un intento de ciberataque	
4. Estaciones y Servidores Mac OS X	4.1. Compatibilidad: 4.1.1. Mac OS X 10.12 o superior 4.1.2. Mac OS X Server 10.9 o superior 4.2. Características: 4.2.1. Debe proporcionar protección residente para archivos (antispyware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado; 4.2.2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota; 4.2.3. La instalación y primera ejecución del producto debe ser realizada sin necesidad de reiniciar la computadora, de modo que el producto funcione en toda su capacidad; 4.2.4. Debe contar con soportes a notificaciones utilizando Growl; 4.2.5. Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo). 4.2.6. Capacidad de volver a la base de datos de la vacuna anterior; 4.2.7. Capacidad de barrer la cuarentena automáticamente después de cada actualización de vacunas; 4.2.8. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de	CUMPLE

Ing. Emidal González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	acuerdo con el resultado del antivirus, (ej.: Win32.Trojan.banker) para que cualquier objeto detectado con el resultado elegido sea ignorado; 4.2.9. Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks); 4.2.10. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo; 4.2.11. Capacidad de verificar solamente archivos nuevos y modificados; 4.2.12. Capacidad de verificar objetos usando heurística; 4.2.13. Capacidad de agendar una pausa en la verificación; 4.2.14. El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe: 4.2.14.1. Preguntar qué hacer, o; 4.2.14.2. Bloquear el acceso al objeto; 4.2.14.2.1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador); 4.2.14.2.2. Caso positivo de desinfección: 4.2.14.2.2.1. Recuperar el objeto para uso; 4.2.14.2.3. Caso negativo de desinfección: 4.2.14.2.3.1. Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador); 4.2.15. Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto; 4.2.16. Capacidad de verificar archivos de formato de correo electrónico; 4.2.17. Posibilidad de trabajar con el producto por la línea de comando, con como mínimo opciones para actualizar las vacunas, iniciar un barrido, para el antivirus e iniciar el antivirus por la línea de comando; 4.2.18. Capacidad de ser instalado, removido y administrado por la misma consola central de gestión;	
5. Estaciones de trabajo Linux	5.1. Compatibilidad: 5.1.1. Debian GNU / Linux 8.9 o superior, x86 / x64 5.1.2. Ubuntu 16.04 LTS o superior, x86 / x64 5.1.3. Linux Mint 18.2 o superior, x86 / x64 5.1.4. ALT, x86 / x64 5.1.5. GosLinux 6.6 o superior, x86 / x64 5.1.6. Mageia 4, x86 5.1.7. Amazon Linux AMI, x64 5.1.8. Astra Linux, x64 5.1.9. OS ROSA Cobalt, x64 5.1.10. AlterOS 7.5 o superior, x64 5.1.11. Pardus OS 19.1 o superior, x64 5.2. Características: 5.2.1. Debe proporcionar las siguientes protecciones: 5.2.1.1. Antivirus de archivos residente (antispyware, antitroyano, antimalware,	CUMPLE

Ing. Emidal González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	antiransomware, análisis de comportamiento y detección de anomalías etc.) que verifique cualquier archivo creado, accedido o modificado; 5.2.1.2. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora. 5.2.2. Capacidad de configurar el permiso de acceso a las funciones del antivirus con, como mínimo, opciones para las siguientes funciones: 5.2.2.1. Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas); 5.2.2.2. Gerenciamiento de respaldo: Creación de copias de los objetos infectados en un reservorio de respaldo antes del intento de desinfectar o eliminar tal objeto, siendo de esta manera posible la recuperación de objetos que contengan informaciones importantes; 5.2.2.3. Gerenciamiento de cuarentena: Cuarentena de objetos sospechosos y corrompidos, guardando tales archivos en una carpeta de cuarentena; 5.2.2.4. Verificación por agendamiento: búsqueda de archivos infectados y sospechosos (incluyendo archivos dentro de un rango especificado); análisis de archivos; desinfección o eliminación de objetos infectados. 5.2.3. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otros software; 5.2.4. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento; 5.2.5. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo; 5.2.6. Capacidad de verificar objetos usando heurística; 5.2.7. Posibilidad de elegir la carpeta donde los archivos recuperados de respaldo y los archivos se grabarán 5.2.8. Posibilidad de elegir la carpeta donde se guardarán los respaldos y archivos en cuarentena 5.2.9. Debe contar con módulo de administración remoto a través de herramienta nativa o Webmin (herramienta nativa GNU-Linux)	
6. Servidores Windows	6.1. Compatibilidad: 6.1.1. Windows Server 2019 todas las versiones 6.1.2. Windows Server 2016 todas las versiones 6.1.3. Windows Server 2012 todas las versiones 6.1.4. Windows Server 2008 todas las versiones, Service Pack 1 o superior 6.1.5. Windows Server 2003 todas las versiones, Service Pack 2 o superior 6.1.6. Windows Storage Server 2012 o superior 6.1.7. Hyper-V Server 2012 o superior 6.1.8. Windows MultiPoint Server 2011 o superior 6.1.9. Small Business Server 2008 o superior	CUMPLE

Ing. Emidal González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	6.2. Características: 6.2.1. Debe proporcionar las siguientes protecciones: 6.2.1.1. Antivirus de archivos residente (antispyware, antitroyano, antimalware, antiransomware, análisis de comportamiento y detección de anomalías etc.) que verifique cualquier archivo creado, accedido o modificado; 6.2.1.2. Autoprotección contra ataques a los servicios/procesos del antivirus 6.2.1.3. Firewall con IDS 6.2.1.4. Control de vulnerabilidades de Windows y de los aplicativos instalados 6.2.2. Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota; 6.2.3. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora. 6.2.4. Capacidad de configurar el permiso de acceso a las funciones del antivirus con, como mínimo, opciones para las siguientes funciones: 6.2.4.1. Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas); 6.2.4.2. Gerenciamiento de tarea (crear o excluir tareas de verificación) 6.2.4.3. Lectura de configuraciones 6.2.4.4. Modificación de configuraciones 6.2.4.5. Gerenciamiento de respaldo y cuarentena 6.2.4.6. Visualización de informes 6.2.4.7. Gerenciamiento de informes 6.2.4.8. Gerenciamiento de claves de licencia 6.2.4.9. Gerenciamiento de permisos (agregar/excluir permisos superiores) 6.2.5. El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas: 6.2.5.1. Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas; 6.2.5.2. Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados. 6.2.6. Capacidad de seleccionar por separado el número de procesos que ejecutarán funciones de barrido en tiempo real, el número de procesos que ejecutarán el barrido a demanda y el número máximo de procesos que pueden ser ejecutados en total. 6.2.7. Capacidad de reanudar automáticamente tareas de verificación que hayan sido interrumpidas por anormalidades (corte de energía, errores, etc.) 6.2.8. Capacidad de automáticamente pausar y no iniciar tareas agendadas en caso de que el servidor esté funcionando con fuente ininterrumpida de energía (uninterruptiblePowersupply UPS)	

Ing. Emidal González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	6.2.9. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otros software; 6.2.10. Capacidad de configurar niveles de verificación diferentes para cada carpeta, grupo de carpetas o archivos del servidor. 6.2.11. Capacidad de bloquear acceso al servidor de máquinas infectadas y cuando una máquina intenta grabar un archivo infectado en el servidor. 6.2.12. Capacidad de crear una lista de máquinas que nunca serán bloqueadas aunque sean infectadas. 6.2.13. Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación; 6.2.14. Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, (ej.: Win32.Trojan.banker) para que cualquier objeto detectado con el resultado elegido sea ignorado; 6.2.15. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento; 6.2.16. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo; 6.2.17. Capacidad de verificar solamente archivos nuevos y modificados; 6.2.18. Capacidad de elegir qué tipo de objeto compuesto será verificado (ej.: archivos comprimidos, archivos autodescompresores, .PST, archivos compactados por compactadores binarios, etc.) 6.2.19. Capacidad de verificar objetos usando heurística; 6.2.20. Capacidad de configurar diferentes acciones para diferentes tipos de amenazas; 6.2.21. Capacidad de agendar una pausa en la verificación; 6.2.22. Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo; 6.2.23. El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe: 6.2.23.1. Preguntar qué hacer, o; 6.2.23.2. Bloquear el acceso al objeto; 6.2.23.2.1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador); 6.2.23.2.2. Caso positivo de desinfección: 6.2.23.2.2.1. Recuperar el objeto para uso; 6.2.23.2.3. Caso negativo de desinfección: 6.2.23.2.3.1. Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador);	

Ing. Emidal González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	6.2.24. Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto. 6.2.25. Posibilidad de elegir la carpeta donde los archivos recuperados de respaldo y los archivos se grabarán 6.2.26. Posibilidad de elegir la carpeta donde se guardarán los respaldos y archivos en cuarentena 6.2.27. Debe contar con módulo que analice cada script ejecutado, buscando señales de actividad maliciosa.	
7. Servidores Linux	1. Compatibilidad: 2. CentOS 6.7 o superior, x86 / x64 3. Red Hat® Enterprise Linux® 6.7 o superior, x64 4. Oracle Linux 7.3 o superior, x64 5. Características: 6. Debe proporcionar las siguientes protecciones: 7. Antivirus de archivos residente (antispyware, antitroyano, antimalware, antiransomware, análisis de comportamiento y detección de anomalías etc.) que verifique cualquier archivo creado, accedido o modificado; 8. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora. 9. Capacidad de configurar el permiso de acceso a las funciones del antivirus con, como mínimo, opciones para las siguientes funciones: 10. Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas); 11. Gerenciamiento de respaldo: Creación de copias de los objetos infectados en un reservorio de respaldo antes del intento de desinfectar o eliminar tal objeto, siendo de esta manera posible la recuperación de objetos que contengan informaciones importantes; 12. Gerenciamiento de cuarentena: Cuarentena de objetos sospechosos y corrompidos, guardando tales archivos en una carpeta de cuarentena; 13. Verificación por agendamiento: búsqueda de archivos infectados y sospechosos (incluyendo archivos dentro de un rango especificado); análisis de archivos; desinfección o eliminación de objetos infectados. 14. En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otro software; 15. Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento; 16. Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del	CUMPLE

Ing. Emidal Gonzalez Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	archivo; 17. Capacidad de verificar objetos usando heurística; 18. Posibilidad de elegir la carpeta donde los archivos recuperados de respaldo y los archivos se grabarán 19. Posibilidad de elegir la carpeta donde se guardarán los respaldos y archivos en cuarentena 20. Debe contar con módulo de administración remoto a través de herramienta nativa o Webmin (herramienta nativa GNU-Linux)	
8. Smartphones y tablets	8.1. Compatibilidad: 8.1.1. Apple iOS 10.0 o superior 8.1.2. Android OS 4.2 o superior 8.2. Características: 8.2.1. Debe proporcionar las siguientes protecciones: 8.2.1.1. Protección en tiempo real del sistema de archivos del dispositivo — interceptación y verificación de: 8.2.1.1.1. Todos los objetos trasmitidos usando conexiones wireless (puerta de infrarrojo, Bluetooth) y mensajes EMS, durante sincronismo con PC y al realizar descargas usando el browser. 8.2.1.1.2. Archivos abiertos en el smartphone 8.2.1.1.3. Programas instalados usando la interface del smartphone 8.2.1.2. Verificación de los objetos en la memoria interna del smartphone y en las tarjetas de expansión a pedido del usuario y de acuerdo con un agendamiento; 8.2.2. Deberá aislar en área de cuarentena los archivos infectados; 8.2.3. Deberá actualizar las bases de vacunas de modo agendado; 8.2.4. Deberá bloquear spam de SMS a través de Black lists (listas negras); 8.2.5. Deberá tener función de bloqueo del aparato en caso de que la SIM CARD sea cambiada por otra no autorizada; 8.2.6. Deberá tener función de limpieza de datos personales a distancia, en caso de robo, por ejemplo. 8.2.7. Deberá tener firewall personal; 8.2.8. Posibilidad de instalación remota utilizando Microsoft System Center Mobile Device Manager 2008 SP1 8.2.9. Posibilidad de instalación remota utilizando SybaseAfaria 6.5 8.2.10. Capacidad de detectar Jailbreak en dispositivos iOS 8.2.11. Capacidad de bloquear el acceso a sitios por categoría en dispositivos 8.2.12. Capacidad de bloquear el acceso a sitios phishing o maliciosos 8.2.13. Capacidad de crear contenedores de aplicativos, separando datos corporativos de datos personales 8.2.14. Capacidad de configurar white y blacklist (listas blancas y listas negras) de aplicativos	CUMPLE
9. Manejo de dispositivos móviles (MDM):	9.1. Compatibilidad: 9.1.1. Dispositivos conectados a través de Microsoft Exchange ActiveSync 9.1.1.1. Apple iOS	CUMPLE

Ing. Ermidal González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	9.1.1.2. Android 9.1.2. Dispositivos con soporte a Apple Push Notification (APNs) service 9.1.2.1. Apple iOS 11.0 o superior 9.2. Características: 9.2.1. Capacidad de aplicar políticas de ActiveSync a través del servidor Microsoft Exchange 9.2.2. Capacidad de ajustar las configuraciones de: 9.2.2.1. Sincronización de correo electrónico 9.2.2.2. Uso de aplicativos 9.2.2.3. Contraseña del usuario 9.2.2.4. Cifrado de datos 9.2.2.5. Conexión de medios extraíbles 9.2.3. Capacidad de instalar certificados digitales en dispositivos móviles 9.2.4. Capacidad de, en forma remota, resetear la contraseña de dispositivos iOS 9.2.5. Capacidad de, en forma remota, borrar todos los datos de dispositivos iOS 9.2.6. Capacidad de, en forma remota, bloquear un dispositivo iOS	
10. Cifrado	10.1. Características: 10.1.1. El acceso al recurso cifrado (archivo, carpeta o disco) debe ser garantizado aún en caso de que el usuario haya olvidado la contraseña, a través de procedimientos de recuperación. 10.1.2. Utilizar, como mínimo, un algoritmo AES con clave de 256 bits. 10.1.3. Capacidad de cifrar completamente el disco duro de la máquina, agregando un ambiente de preboot para autenticación del usuario. 10.1.4. Capacidad de utilizar Single Sign-On para la autenticación de preboot. 10.1.5. Permitir crear varios usuarios de autenticación preboot. 10.1.6. Capacidad de crear un usuario de autenticación preboot común con una contraseña igual para todas las máquinas a partir de la consola de manejo. 10.1.7. Capacidad de cifrar drives extraíbles de acuerdo con una regla creada por el administrador, con las opciones: 10.1.7.1. Cifrar solamente los archivos nuevos que sean copiados para el disco extraíble, sin modificar los archivos ya existentes. 10.1.7.2. Cifrar todos los archivos individualmente. 10.1.7.3. Cifrar el dispositivo entero, de manera que no sea posible listar los archivos y carpetas almacenadas. 10.1.7.4. Cifrar el dispositivo en modo portátil, permitiendo acceder a los archivos en máquinas de terceros a través de una contraseña. 10.1.8. Capacidad de seleccionar carpetas y archivos (por tipo, o extensión) para ser cifradas automáticamente. En esta modalidad, los archivos deben estar accesibles para todas las máquinas gestionadas por la misma consola de manera transparente para los usuarios. 10.1.9. Capacidad de crear reglas de exclusiones para que ciertos archivos o carpetas nunca sean cifrados.	CUMPLE

Ing. Emidal González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - I

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	10.1.10. Capacidad de seleccionar aplicaciones que pueden o no tener acceso a los archivos cifrados.	
11. Gerenciamiento de Sistemas	11.1. Capacidad de crear imágenes de sistema operativo remotamente y distribuir esas imágenes para computadoras gestionadas por la solución y para computadoras bare-metal. 11.2. Capacidad de detectar software de terceros vulnerables, creando así un informe de software vulnerables. 11.3. Capacidad de corregir las vulnerabilidades de software, haciendo el download centralizado de la corrección o actualización y aplicando esa corrección o actualización en las máquinas gestionadas de manera transparente para los usuarios. 11.4. Capacidad de gestionar licencias de software de terceros. 11.5. Capacidad de registrar cambios de hardware en las máquinas gestionadas. 11.6. Capacidad de gestionar un inventario de hardware, con la posibilidad de registro de dispositivos (ej.: router, switch, proyector, accesorio, etc.), informando fecha de compra, lugar donde se encuentra, servicetag, número de identificación y otros.	CUMPLE
12. Servidores de correo electrónico Windows	12.1. Características: 12.1.1. Debe utilizar las tecnologías VSAPI 2.0, 2.5 y 2.6; 12.1.2. Capacidad de iniciar varias copias del proceso de antivirus; 12.1.3. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora. 12.1.4. Capacidad de verificar carpetas públicas, correos electrónicos enviados, recibidos y almacenados contra virus, spywares, adwares, gusanos, troyanos y riskwares; 12.1.5. Capacidad de verificar carpetas públicas y correos electrónicos almacenados de forma agendada, utilizando las últimas vacunas y heurística; 12.1.6. El antivirus, al encontrar un objeto infectado, debe: 12.1.6.1. Desinfectar el objeto, notificando el remitente, destinatario y administradores, o 12.1.6.2. Excluir el objeto, sustituyéndolo por una notificación; 12.1.6.3. Bloquear el acceso al objeto; 12.1.6.3.1. Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador); 12.1.6.3.2. Caso positivo de desinfección: 12.1.6.3.2.1. Recuperar el objeto para uso; 12.1.6.3.3. Caso negativo de desinfección: 12.1.6.3.3.1. Mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador); 12.1.7. Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto. 12.1.8. Capacidad de enviar notificaciones sobre virus detectados para el administrador, para el destinatario y remitente del mensaje infectado. 12.1.9. Capacidad de grabar logs de actividad de virus en los eventos del sistema y en los logs	CUMPLE

Ing. Emidio González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	internos de la aplicación; 12.1.10. Capacidad de detectar diseminación en masa de correos infectados, informando al administrador y registrando tales eventos en los logs del sistema y de la aplicación.	
13. Servidores de correo electrónico Lotus Notes/Domino	13.1. Características: 13.1.1. Capacidad de barrido de banco de datos internos del sistema Lotus Notes/Domino; 13.1.2. Capacidad de barrido en las réplicas de otros servidores Domino que no tengan el antivirus instalado; 13.1.3. Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora. 13.1.4. Capacidad de barrido de virus en todos los correos electrónicos que pasan por el sistema Lotus Notes/Domino; 13.1.5. El barrido debe involucrar el texto del mensaje y los archivos adjuntos; 13.1.6. Capacidad de cura de mensajes infectados; 13.1.7. Capacidad de filtrado de archivos por tipo; 13.1.8. Capacidad de creación de cuarentena para objetos sospechosos, evitando pérdida de datos; 13.1.9. Capacidad de notificación del destinatario, remitente y administrador sobre objetos que contengan archivos maliciosos; 13.1.10. Capacidad de detección de epidemias y notificaciones de estos eventos al administrador; 13.1.11. Capacidad de actualización vía HTTP, FTP o carpeta en red local; 13.1.12. Capacidad de configurar el tamaño máximo de un archivo que será verificado;	CUMPLE
14. Servidores de correo electrónico Linux	14.1. Características: 14.1.1. Capacidad de verificar el tráfico SMTP del servidor contra malware en todos los elementos del correo electrónico: encabezado, cuerpo y adjunto; 14.1.2. Capacidad de notificar al administrador, al remitente y al destinatario en caso de que un archivo malicioso sea encontrado en el correo electrónico; 14.1.3. Capacidad de poner en cuarentena objetos maliciosos; 14.1.4. Capacidad de guardar respaldo de los objetos antes del intento de desinfección; 14.1.5. Capacidad de hacer barrido en el sistema de archivos del servidor; 14.1.6. Capacidad de filtrar adjuntos por nombre o tipo de archivo; 14.1.7. Capacidad de crear grupos de usuarios para aplicar reglas de verificación de correos electrónicos; 14.1.8. Debe permitir gestión vía consola WEB; 14.1.9. Debe ser actualizado de manera automática vía internet o por servidores locales, con frecuencia horaria.	CUMPLE
15. Funcionalidades de Detección y Respuesta de Endpoints	15.1. La solución debe operar mediante una única consola tanto en entorno local como en la nube. 15.2. La solución debe incluir módulos EDR	CUMPLE

Ing. Emidal González Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

ESPECIFICACIONES TÉCNICAS		Corporation Sekiura S.A.C.E.I
	15.3. La solución debe contar con funciones de automatización que garanticen la solución rápida de incidentes. 15.4. Capacidad de visualización de alertas de seguridad de los endpoints 15.5. Capacidad de configurar respuestas automatizadas para amenazas descubiertas en todos los endpoints basadas en exploraciones de indicadores de compromiso - IoC 15.6. Capacidad de respuesta instantánea a incidentes tras el descubrimiento 15.7. Las opciones de respuesta deben incluir: 15.7.1. aislar el host 15.7.2. poner en cuarentena el archivo 15.7.3. iniciar el análisis del host 15.7.4. impedir que se ejecute el archivo. 15.8. Capacidad de brindar información acerca de: 15.8.1. Alcance de la amenaza. 15.8.2. Estado de la amenaza: activo y desactivado. 15.8.3. Identificación de los hosts y cuentas de usuarios afectados. 15.8.4. Origen de la amenaza. 15.9. Capacidad de neutralizar amenazas mediante respuesta automática. 15.10. Capacidad de reacción inmediata a los incidentes detectados.	
16. Soporte técnico que incluya	16.1. El proveedor deberá bridar soporte técnico insitu 24/7 durante el período de licencias; además de dar un adiestramiento mínimo de 40 horas en el uso de la herramienta a 4 personas de la institution. 16.2. Cantidad de tickets de soporte ilimitados. 16.3. Actualización de la consola, agentes y endpoints. 16.4. Actualización de versiones de Sistemas Operativos. 16.5. Respuesta ante incidents. 16.6. Administración de parches de seguridad. 16.7. Análisis forense e indicadores de compromiso. 16.8. Informes semanales de eventos de seguridad. 16.9. Implementación de todos los módulos de la herramienta en todo el parque de equipos 16.10. El proveedor deberá contar con una plataforma y/o sistema de ticket para atención de casos de soporte técnico, a fin de garantizar la respuesta de manera profesional y organizada. 16.11. El proveedor local deberá contar con una plataforma de autoservicio de preguntas frecuentes, con por lo menos 50 plantillas de respuesta para esos casos, dicha plataforma deberá estar integrada con el sistema del ticket del proveedor	CUMPLE

Ing. Emidal Gonzalez Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS

INFORME DE EVALUACIÓN TÉCNICA

LPN 36/2023 ADQUISICIÓN DE RENOVACIÓN Y ACTUALIZACIÓN DE SOFTWARE DE SEGURIDAD, CONTROL DE PUNTO FINAL, DETECCIÓN Y RESPUESTA ANTE INCIDENTES Y PROTECCIÓN DE CORREO ELECTRÓNICO PARA EL MSPYBS- AD REFERENDUM"- PLURIANUAL

CAPACIDAD TÉCNICA		Corporation Sekiura S.A.C.E.I
17. Capacidad Técnica del Oferente:	17.1. Contar con por lo menos 1 técnico con certificación CEH y CEH MASTER 17.2. Contar como mínimo con 2 técnicos certificados con las certificaciones avanzadas del producto 17.3. Contar como mínimo con 2 técnicos con certificaciones de cifrado 17.4. Contar con por lo menos 2 técnicos con certificaciones en protección de servidores de correo antispam 17.5. Contar con por lo menos 2 técnicos con certificaciones en Detección y Respuesta de Endpoints 17.6. Los técnicos certificados deben ser personales dependientes de la Empresa Oferente, se deben acompañar certificados de inscripción en IPS 17.7. Contar como mínimo con 2 técnicos con certificaciones ITIL para garantizar la buena asistencia en soporte técnico. 17.8. Contar con al menos 10 contratos o facturas de la provisión del Software ofertado entre los años 2019, 2020 y 2021. 17.9. El proveedor deberá ser Canal Platinum de la Marca ofertada, para garantizar el buen servicio y respaldo del soporte local. 17.10. 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. 17.11. El proveedor deberá presentar una autorización del fabricante expresamente dirigido a la convocante refiriendo el nro. de ID del llamado 17.12. La convocante podrá solicitar si cree necesario a los oferentes una demostración del manejo y despliegue de la herramienta	CUMPLE

Ing. Emidal Gonzalez Aguilera
Director
Dirección de Seguridad Informática
DGTIC - MSP y BS