INFORME TÉCNICO DE ESTANDARIZACIÓN N° 002-2021-MINEDU/SPE-OTIC

"ESTANDARIZACIÓN DE SOLUCIÓN DE ANTIVIRUS CORPORATIVO PARA EL MINISTERIO DE EDUCACIÓN"

1. DESCRIPCIÓN DE LA INFRAESTRUCTURA PREEXISTENTE

El Ministerio de Educación (MINEDU), a través de la Oficina de Tecnologías de la Información y Comunicación, ha implementado una infraestructura de seguridad a nivel endpoint (solución de antivirus) para los equipos de cómputo utilizados por los usuarios del MINEDU para prevenir y brindar protección ante amenazas, virus, malware, adware, gusanos, troyanos, entre otros, tanto en la sede central como en sedes desconcentradas a cargo del MINEDU.

La implementación de esta infraestructura de seguridad fue realizada como parte de la adquisición realizada mediante Licitación pública N° 1-2018-MINEDU/UE.024 "ADQUISICIÓN DE SOLUCIÓN ANTIVIRUS PARA LA SEDE CENTRAL Y DEPENDENCIAS DEL MINISTERIO DE EDUCACIÓN".

La solución de seguridad a nivel de endpoint implementada en el MINEDU constituye una solución preexistente de la marca Kaspersky, ya que se encuentran instalados en los equipos de cómputo que forman parte de las diferentes sedes a cargo del MINEDU, los cuales se encuentran gestionados por sus respectivas consolas de administración. La relación del licenciamiento con el que cuenta el MINEDU para brindar esta protección a nivel endpoint es la siguiente:

NOMBRE DEL PRODUCTO	ID DE LICENCIA	CANTIDAD	FECHA DE EXPIRACIÓN
Kaspersky Endpoint Security for Business Advanced	1E3A-181004-191330-133-1129	4000 NODOS	06/02/2022
Kaspersky Endpoint Detection and Response Advanced Edition	1E3A-180929-023630-623-1034	4000 NODOS	06/02/2022

2. DESCRIPCIÓN Y USO QUE SE DARÁ A LOS BIENES Y SERVICIOS REQUERIDOS

La solución de antivirus que tiene el MINEDU, destinada a equipos de cómputo, de la marca Kaspersky permite realizar las siguientes funcionalidades que han sido personalizadas y optimizadas, según las necesidades de protección que se requiere en los equipos de cómputo del MINEDU:

Protección ante amenazas: Permite brindar protección a una amplia gama de amenazas que intentan infectar a los equipos de cómputo, dentro de los cuales se encuentran: virus, malware, adware, troyanos, gusanos, ransomware, así como de intentos de intrusiones, amenazas de red, entre otros, ya que no solo está basado en firmas, sino también funciona en base a comportamiento y otros tipos de técnicas que permiten brindar la protección requerida.

Protección de correo electrónico: Permite interactuar con el cliente de correo electrónico para proteger los equipos de cómputo de phishing y archivos adjuntos infectados.
Control de aplicaciones: Permite tener el control de las aplicaciones que pueden hacer uso los usuarios. Cuenta con la configuración y personalización de las aplicaciones que se encuentran prohibidas por política de seguridad, en los equipos de cómputo de los

usuarios, así como las excepciones que son permitidas en base a las autorizaciones brindadas.

Control web: Permite realizar las configuraciones de las categorías a las que tienen permitidas las navegaciones de los usuarios, tanto las relacionadas con seguridad como las relacionadas con productividad en la utilización a internet, de tal modo que no generen un tráfico excesivo en el uso del recurso de internet. Así mismo cuenta con la configuración y personalización de excepciones de páginas web necesarias para la utilización de las labores administrativas y pedagógicas de los usuarios.

Detección de vulnerabilidades: Permite detectar las aplicaciones instaladas en los equipos de cómputo, independientemente de la marca de dichas aplicaciones, e identificar cuáles son las que se encuentran vulnerables, brindando adicionalmente la opción de corregir dichas vulnerabilidades, ya sea de manera automática o programada.

Administración mediante consola centralizada: Permite la administración de la solución de antivirus, con la capacidad de identificar de forma automática los equipos de cómputo conectados a la red institucional, realizar configuraciones de: instalación de la solución de seguridad a nuevos equipos conectados a la red, envío de actualizaciones de firmas periódicos, de protección en tiempo real y de envíos periódicos de análisis y detección de amenazas, políticas personalizadas, inventario de hardware, de software; así mismo, permita generar y mostrar el detalle de eventos como: errores generados en la actualización, amenazas detectadas y las acciones/correcciones/mitigaciones realizadas a dichas amenazas, tareas realizadas, con sus respectivos reportes configurables y personalizables, que permiten la ejecución manual así como el envío automático por correo electrónico en formatos como csv, pdf, etc.

EDR: Brinda visibilidad detallada de los eventos generados respecto a posibles amenazas nuevas, desconocidas, ocurridas en los equipos de cómputo, con la finalidad de inspeccionar dicho comportamiento y tomar las acciones preventivas o de corrección que se requieran. Además, se incluye Sandbox que permita realizar el análisis mediante la detonación de las nuevas amenazas detectadas y tomar acción en base al resultado obtenido.

El MINEDU requiere contar de forma continua con la protección de seguridad a nivel endpoint mediante una solución de antivirus que no consuma muchos recursos, pero a la vez sea estable, de calidad y brinde la protección de seguridad avanzada que requiere la entidad ante constantes amenazas que intentan ingresar a los equipos del MINEDU por la red, internet, correo electrónico, medios extraíbles, etc.

La estandarización de la solución de antivirus con las que cuenta el MINEDU de la marca Kaspersky (solución que incluya como mínimo los componentes: EPP, EDR y Sandbox, o equivalente a dicha solución) permitirá contar con la protección a nivel de seguridad que se requiere, y a la vez garantizar la compatibilidad con las configuraciones ya realizadas como cumplimiento de las políticas de seguridad establecidas para la protección de los equipos de cómputo, así como para las exclusiones generadas ante las solicitudes y requerimientos realizados por las diversas oficinas usuarias del MINEDU; ya que el licenciamiento de la solución de antivirus con la que cuenta el MINEDU fue adquirido en el año 2018, con lo que solo requeriría:

- La renovación de la solución de antivirus para la actualización de nuevas firmas, así como detección y protección ante nuevas amenazas existentes en el tiempo.
- Y al estandarizar la solución de antivirus, es necesario la estandarización del soporte y garantía de dicho licenciamiento, ante posibles fallas.

En caso no se realice la estandarización, se requeriría adquirir una nueva solución que brinde la misma funcionalidad que la solución de antivirus que actualmente tiene el MINEDU y adicionalmente tiene que realizarse la implementación en todos los equipos de cómputo del MINEDU y en caso no sea posible implementarlo de forma remota, se tendría que ubicar dichos equipos en las diferentes sedes del MINEDU para poder

brindar la protección necesaria. Adicionalmente se tendría que tener una etapa de aprendizaje de la red y aplicaciones que utilizan los usuarios, así como la reconfiguración de las políticas de seguridad y excepciones aplicadas actualmente. A ello se suma la capacitación del uso de una nueva solución de seguridad. Todo ello generaría incomodidad a las operaciones que realizan los usuarios para cumplir con sus labores administrativas y pedagógicas, así como mayores costos a la entidad.

Teniendo en cuenta lo indicado, la solución de antivirus con la que cuenta el MINEDU para la protección de los equipos de cómputo fue adquirida por la entidad y no ha presentado inconvenientes, por el contrario, ha permitido la optimización de la configuración de las políticas de seguridad del MINEDU, por lo que se requiere estandarizar la solución de antivirus de la marca Kaspersky, de tal modo que permita realizar la adquisición/renovación del licenciamiento, soporte y garantía de dicha solución, con lo cual será posible prolongar el tiempo de vida/periodo de utilización del licenciamiento adquirido por el MINEDU en el año 2018, lo que permitirá que los equipos de cómputo continúen con la protección deseada, tengan un máximo desempeño a las funcionalidades con las que se cuenta y los equipos se encuentren disponibles, sin impacto para los usuarios.

Por ello, para poder dar continuidad a la protección de seguridad de los equipos de cómputo con la solución de antivirus de la marca Kaspersky, es necesario lo siguiente:

a) Estandarizar la solución de antivirus de la marca Kaspersky, que incluya como mínimo los siguientes componentes:
   - EPP (Kaspersky Endpoint Security for Business Advanced); o equivalente.
   - EDR (Kaspersky Endpoint Detection and Response Advanced), que incluya la licencia para Kaspersky Sandbox; o equivalente.

b) Estandarizar el soporte técnico para la solución de antivirus de la marca Kaspersky, que permita la creación de ticket, atención y solución de casos; o equivalente.

3. JUSTIFICACIÓN DE LA ESTANDARIZACIÓN

Atendiendo a las normas legales señaladas en el literal d) del numeral VII. 7.3 de la Directiva N° 004-2016-OSCE/CD "*Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular*", el Ministerio de Educación cumple con lo señalado en dicho documento, conforme se indica a continuación:

El Ministerio de Educación busca proteger la inversión en las implementaciones realizadas con anterioridad respecto a la solución de antivirus, así como a las implementaciones futuras, con el fin de asegurar la funcionalidad óptima de la protección de los equipos de cómputo, mediante la continuidad de las características y configuraciones de la solución de antivirus de la marca Kaspersky.

La solución de antivirus en los equipos de cómputo viene a ser la primera capa de seguridad institucional, siendo una medida de protección fundamental para la seguridad institucional, ya que protege ante amenazas que vienen por diferentes medios como la red, internet, dispositivos extraíbles, aplicaciones vulneradas, por lo que tiene configuraciones personalizadas que permiten la protección a nivel de internet, clientes de correo electrónico, uso de aplicaciones, entre otros.

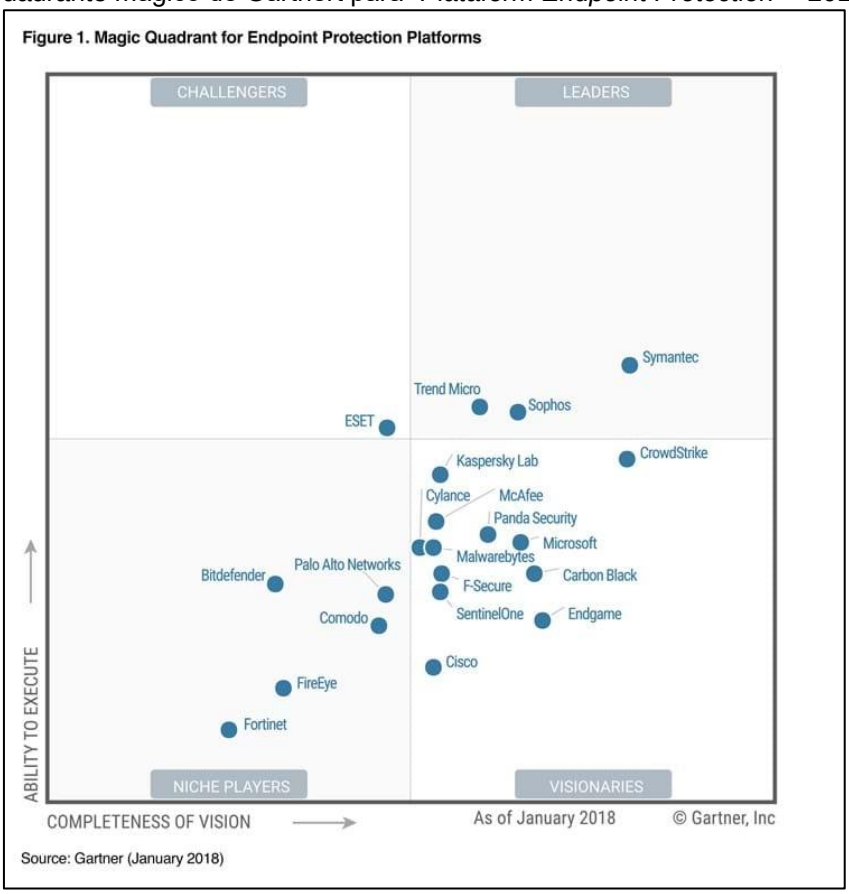
La implementación que se tiene para la solución de antivirus tiene protección con contraseña para evitar la desinstalación o manipulación en su configuración, impidiendo que usuarios quiten o modifiquen la protección brindada, lo cual constituye en la optimización de los mecanismos de seguridad.

Así mismo, el personal que administra la solución de antivirus tiene conocimiento, se encuentra entrenado y cuenta con la experiencia en la instalación, configuración y administración de la misma, de tal modo que en caso de presentarse eventos o errores en la configuración o incidencias, existirá personal en la entidad como primera línea para solucionar dichos inconvenientes relacionados a la solución de antivirus.

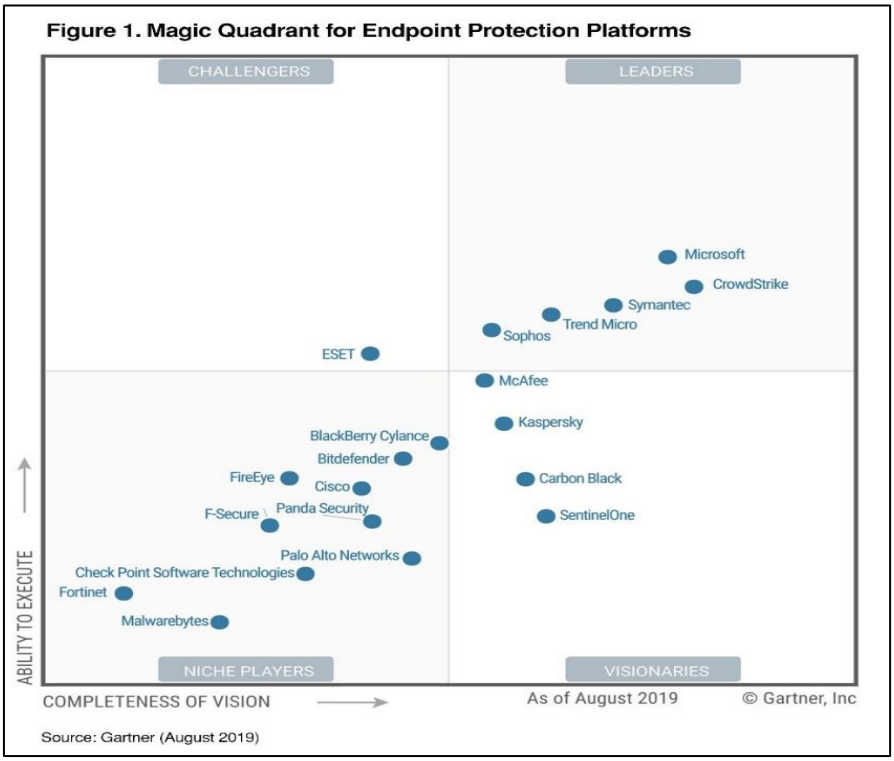
En el mercado existen diversas marcas de soluciones de antivirus; sin embargo, la entidad en los últimos años viene utilizando de manera eficiente la solución de antivirus de la marca Kaspersky, ya que cuenta con opciones avanzadas de seguridad, permitiendo un alto nivel de protección contra una amplia gama de amenazas.

Según el cuadrante mágico de Gartnert para "*Plataform Endpoint Protection*" en los últimos años (siendo los 3 últimos reportes los correspondientes a los años: 2018, 2019 y 2021), la marca Kaspersky de manera consecutiva se encuentra en el cuadrante de "visionarios", tal como se muestra a continuación:

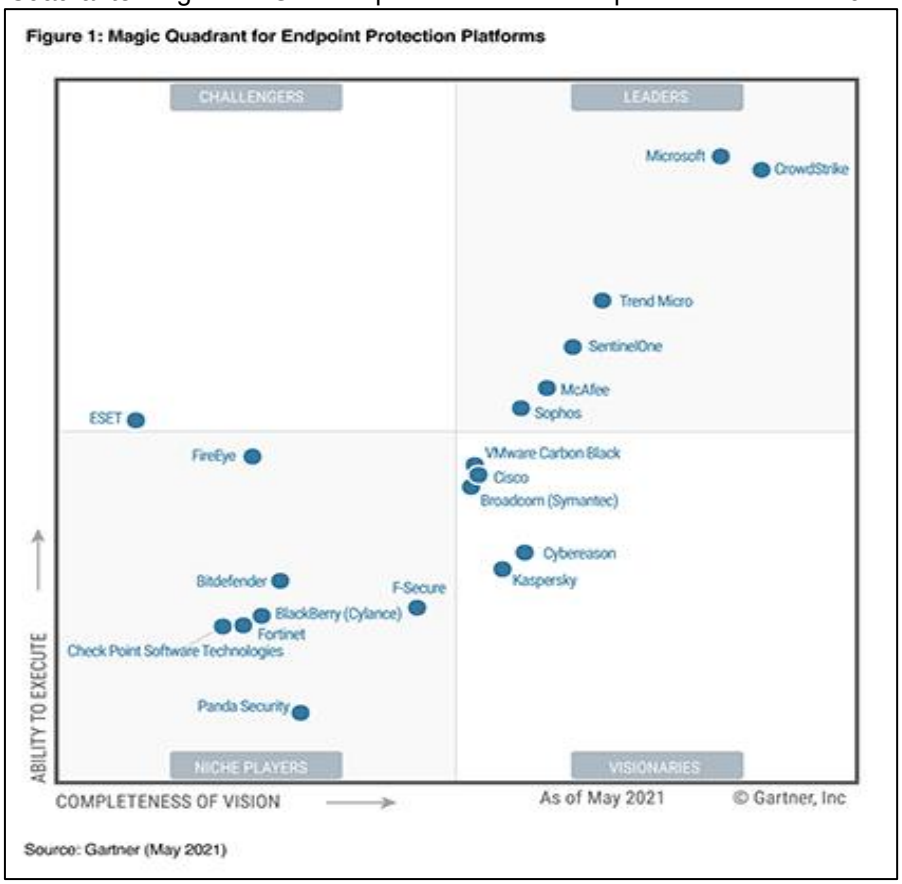
Cuadrante mágico de Gartnert para "*Plataform Endpoint Protection*" - 2018



Cuadrante mágico de Gartnert para "*Plataform Endpoint Protection*" - 2019



Cuadrante mágico de Gartnert para "Plataform Endpoint Protection" - 2021



a) La Entidad posee determinado equipamiento o infraestructura, pudiendo ser maquinarias, equipos, vehículos, u otro tipo de bienes, así como ciertos servicios especializados:

Desde el año 2018 el Ministerio de Educación adquirió, implementó y puso en funcionamiento la solución de antivirus de la marca Kaspersky para los equipos de cómputo, constituida por las licencias de los productos: Kaspersky Endpoint Security for Business Advanced y Kaspersky Endpoint Detection and Response que incluye Sanbox, que brinda protección a nivel de endpoint, ante amenazas existentes, nuevas amenazas, control web, control de aplicaciones, control de vulnerabilidades, entre otros, los que son gestionados mediante sus respectivas consolas de administración de la seguridad de los equipos de cómputo que permite: el control, seguimiento, detección de eventos, identificación de origen de amenazas y seguimiento de archivos posiblemente comprometidos con el fin de tomar acciones de mitigación de manera automática o personalizada, generación de reportes, entre otros, licenciamiento que permite contar con la actualización de firmas de protección y nuevas versiones por el periodo de tres (03) años.

Adicionalmente se cuenta con el soporte y garantía de la solución de antivirus de la marca Kaspersky (para los mismos productos adquiridos), por el periodo de tres (03) años.

La vigencia para las actualizaciones de firmas, nuevas versiones, soporte y garantía es hasta el día 05 de febrero del 2022.

b) Los bienes o servicios que se requiere contratar son accesorios o complementarios al equipamiento o infraestructura preexistente:

La solución de antivirus que actualmente se utiliza en el MINEDU para los equipos de cómputo constituye el primer nivel de los esquemas de seguridad con los que se cuentan en el MINEDU, en cumplimiento de las políticas de seguridad institucionales.

El licenciamiento que permite el funcionamiento de la solución de antivirus fue adquirido e implementado en los equipos de cómputo de las diferentes sedes del MINEDU desde el año 2018, teniendo configuraciones y personalizaciones de seguridad en base a los requerimientos y necesidades de los usuarios de las diferentes sedes del MINEDU.

Con la adquisición de los nuevos equipos de cómputo con el que se está renovando el parque tecnológico del MINEDU, instalados en los años 2020 y 2021, la solución de antivirus ha sido implementada también en los nuevos equipos de cómputo, con todas las configuraciones y políticas respectivas.

Por ello, para continuar brindando la protección de seguridad a los equipos de cómputo del MINEDU, los cuales ya cuentan con la solución de antivirus instaladas, configuradas y con las personalizaciones que permiten a los usuarios realizar sus actividades diarias, se requiere contar de forma complementaria con la renovación del licenciamiento del antivirus con el que cuenta el MINEDU, siendo para ello necesaria la estandarización de dicho licenciamiento, soporte y garantía respectivos o equivalente.

c) Los bienes o servicios que se requiere contratar son imprescindibles para garantizar la funcionalidad, operatividad o valor económico del equipamiento o infraestructura preexistente:

La protección de la información que tienen los equipos de cómputo, así como las aplicaciones que utilizan los usuarios del MINEDU, es de vital importancia para cumplir con los objetivos estratégicos institucionales.
Para brindar dicha protección, la primera capa de seguridad mínima que todo equipo de cómputo debe tener corresponde a una solución de antivirus.

Debido a que el MINEDU ya cuenta con la solución de antivirus para equipos de cómputo de marca Kaspersky, la cual viene funcionando de manera eficiente debido a que tiene opciones avanzadas de seguridad, permitiendo un alto nivel de protección contra una amplia gama de amenazas, la estandarización de dicha solución permitirá que al renovar el licenciamiento sea posible contar con las nuevas firmas de seguridad y las actualizaciones de nuevas versiones que puedan existir en el tiempo, único mecanismo mediante el cual puede ser utilizada la infraestructura lógica de seguridad a nivel endpoint implementada en los equipos de cómputo del MINEDU y esta pueda seguir operando y funcionando, garantizando con ello la continuidad de la protección de la información institucional y cumplimiento de las políticas de seguridad institucionales.

Con esta estandarización no solo será posible seguir utilizando la infraestructura lógica a nivel de endpoint existente en el MINEDU, sino que además evitará que se tenga que realizar una nueva implementación a todos los equipos de cómputo del MINEDU con una solución de antivirus diferente y el riesgo que esto implica respecto a incompatibilidades que pudieran existir con aplicaciones que utilizan los usuarios del MINEDU, cuyas personalizaciones ya se encuentran optimizadas con la actual solución de antivirus.

Así mismo, en caso el parque tecnológico del MINEDU crezca, la estandarización del antivirus permitirá, que al necesitar proteger los equipos de cómputo adicionales con los que cuente la entidad, se continúen teniendo la misma protección de antivirus institucional, con las configuraciones y personalizaciones de las políticas de seguridad establecidas.

d) Incidencia económica de la contratación:

Debido a que ya se encuentra implementada la solución de antivirus para equipos de cómputo, la estandarización solicitada no requerirá de instalaciones o implementaciones de dicha solución en los equipos de cómputo del MINEDU, por lo que con ello se evitaría los gastos de implementación que podrían originarse si es que no se estandariza la solución de antivirus solicitada, la incomodidad que generaría a los usuarios la desinstalación de la solución de antivirus actual y la instalación de otras marcas de antivirus, así como la ventana de aprendizaje que requeriría la nueva solución de antivirus respecto a incompatibilidades que pudieran existir con aplicaciones que utilizan los usuarios.

Por otro lado, debido a que el personal se encuentra capacitado y con la experiencia en el funcionamiento y operatividad de la solución de antivirus con el que cuenta la entidad, se evitaría los gastos de capacitación si es que no se estandariza la solución de antivirus solicitada.

Adicionalmente a lo indicado se precisa que de no estandarizar la solución de antivirus Kaspersky, se necesitaría la adquisición de una solución de antivirus de una marca diferente.

La incidencia económica del licenciamiento de la solución de antivirus a estandarizar y de otras opciones alternativas que se ajustan a las características mínimas solicitadas, basadas en cotizaciones referenciales, así como el análisis costo beneficio se indican a continuación:

Marca de la solución de antivirus	Costo de licencias	Beneficio	Beneficio/Costo
FSECURE	S/ 247.80	83	85%
KASPERSKY	S/ 514.48	98	93%
MCAFEE	S/ 400.00	88	85%

Por lo tanto, tal como se indica en el Informe Técnico Previo de Evaluación de Software N° 006-2021-MINEDU/SPE-OTIC - "SOLUCIÓN DE ANTIVIRUS CORPORATIVO PARA EL MINISTERIO DE EDUCACIÓN", del análisis realizado a diversas soluciones de antivirus que existen en el mercado y que cubren con las características mínimas de seguridad y calidad que se requieren en la entidad, así como de su relación costo-

beneficio se obtiene que la solución de antivirus de la marca Kaspersky es la mejor alternativa para las necesidades del MINEDU, cuya evaluación fue realizada bajo los estándares de la "*Guía Técnica sobre evaluación de software en la Administración Pública*" tal como se exige en el reglamento de la Ley N° 28612.

e) Periodo de vigencia:

El periodo de vigencia para la estandarización de licencias, soporte y garantía de la solución de antivirus de la marca Kaspersky es de tres (03) años. De presentarse el caso que las condiciones que determinan esta estandarización varíen, dicha aprobación quedará sin efecto.

4. CONCLUSIONES

Debido a que el MINEDU cuenta con una solución de antivirus como infraestructura preexistente, mediante la cual brinda niveles de seguridad de calidad y tiene establecidos configuraciones personalizadas, con la finalidad que pueda seguir operando y funcionando, garantizando con ello la continuidad de la protección de la información institucional y cumplimiento de las políticas de seguridad institucionales, se recomienda la estandarización de la solución de antivirus de la marca Kaspersky, correspondiente al licenciamiento, soporte y garantía o equivalente.

5. RESPONSABLES DE LA EVALUACIÓN

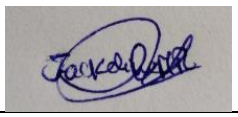
Las personas responsables de la evaluación que sustentan la elaboración del presente informe son:

- La sra. Jackeline Johana Melgarejo Reyes - Especialista del área de Comunicaciones y Seguridad Lógica de la UIT - OTIC.
- El sr. Jorge John Trujillo Ramirez - Coordinador del área de Comunicaciones y Seguridad Lógica de la UIT - OTIC.
- El sr. Aldo Humberto Amaya Ysla – Jefe (e) de la Unidad de Infraestructura Tecnológica (UIT) - OTIC.
- El sr. Max Ever Ponce Soldevilla - Jefe de la Oficina de Tecnologías de la Información y Comunicación (OTIC).

6. FECHA DE ELABORACIÓN

Octubre del 2021.

7. FIRMAS



JACKELINE JOHANA MELGAREJO REYES
Especialista del área de Comunicaciones y Seguridad Lógica de la UIT - OTIC

JORGE JOHN TRUJILLO RAMIREZ
Coordinador del área de Comunicaciones y Seguridad Lógica de la UIT - OTIC

FIRMA DIGITAL
Firmado digitalmente por: AMAYA YSLA Aldo Humberto FAU 20131370998 soft
Motivo: En señal de conformidad
Fecha: 15/10/2021 23:53:44-0500

ALDO HUMBERTO AMAYA YSLA
Jefe (e) de la Unidad de Infraestructura Tecnológica (UIT) - OTIC

MAX EVER PONCE SOLDEVILLA
Jefe de la Oficina de Tecnologías de la Información y Comunicación (OTIC)

FIRMA DIGITAL
Firmado digitalmente por: PONCE SOLDEVILLA Max Ever FAU 20131370998 hard
Motivo: Soy el autor del documento
Fecha: 19/10/2021 10:19:32-0500

FIRMA DIGITAL
Firmado digitalmente por: TRUJILLO RAMIREZ Jorge John FAU 20131370998 soft
Motivo: En señal de conformidad
Fecha: 15/10/2021 23:51:26-0500