INFORME TÉCNICO DE EVALUACIÓN DE SOFTWARE DE ADQUISICIÓN DE LICENCIAS DE ANTIVIRUS PARA EL MINISTERIO DE TRANSPORTES Y COMUNICACIONES

INFORME TÉCNICO N° 0015-2017-MTC/10.06.LRBS

1 NOMBRE DEL ÁREA

OFICINA DE TECNOLOGÍA DE INFORMACIÓN

2 RESPONSABLE DE LA EVALUACIÓN

PATRICK MUÑANTE LOAYZA

LUIS ROBERTO BLAS SERNAQUE

3 CARGO

ANALISTA DE SEGURIDAD INFORMÁTICA

ESPECIALISTA NORMATIVO Y REGULACIÓN DE TI

4 FECHA

21/02/2017

5 JUSTIFICACIÓN

El Ministerio de Transportes y Comunicaciones (MTC), cuenta con un parque de equipos de cómputo operativos, los cuales requieren contar con un software capaz de brindar protección a través de una licencia corporativa de antivirus para la protección de la información ante la amenaza de programas con código malicioso virus, spyware, malware que ingresan por Internet o mediante dispositivos removibles como USB.

Actualmente, se tiene un déficit de licencias antivirus que brinda la protección y seguridad a la información institucional para las computadoras personales, además que permita la aplicación de control de acceso a dispositivos removible.

6 ALTERNATIVAS

Considerando la Importancia de contar con una plataforma de administración que permita la gestión y monitoreo de los servicios, se han determinado las siguientes alternativas:

Ítem	Producto
1	Kaspersky EndPoint Security Business – Advanced
2	Symantec Endpoint Protection Suite
3	Trend Micro Security
4	Intel Security (antes McAfee).

Para la evaluación técnica, se tienen los siguientes supuestos:

a) Presentaciones de los representantes de las empresas proveedoras de soluciones de software.
b) La información disponible en la página web de cada uno de los fabricantes.
c) Información disponible en Internet.

d) Cuadrante de Gartner, ver Anexo 1.
e) Evaluaciones similares en otras instituciones del Estado Peruano.

Es importante remarcar que los productos Kaspersky, Symantec, Trend Micro e Intel Security son de tipo Propietario.

7 ANÁLISIS COMPARATIVO TÉCNICO

El análisis comparativo técnico está basado en la metodología establecida en la Guía Técnica sobre Evaluación de Software para la Administración Pública, aprobada por Resolución Ministerial N° 139-2004-PCM.

7.1 Propósito de la Evaluación

Identificar características de calidad mínima de la solución de antivirus.

7.2 Identificar el tipo de software

Se aplica el modelo establecido en la Guía Técnica sobre Evaluación de Software para la Administración Pública (R.M. N° 139-2004-PCM).

7.3 Especificación del Modelo de Calidad

Se aplicará el modelo de calidad de software descrito en la parte 1 de la Guía de evaluación de software aprobada por R.M N° 139-2004-PCM y la Ley N° 28612 - "Ley que norma el uso, adquisición y adecuación del software en la administración pública".

7.4 Selección de métricas

La selección de métricas se obtuvo a partir de los atributos especificados en el Modelo de Calidad, tal como se detalla en el **Anexo N°2: "Atributos de evaluación de software".**

Para cuantificar cada uno los requisitos o requerimientos se ha asignado un valor de acuerdo al siguiente cuadro:

Detalle	Valor
Cumplimiento de requisito a nivel Alto	5
Cumplimiento de requisito a nivel Medio	4
Cumplimiento de requisito a nivel Bajo	3

Considerando que la suma de los puntajes máximos es 100 para la evaluación de alternativas, se considerará la siguiente tabla de aceptación de alternativas, para la provisión del sistema de seguridad evaluado para el MTC.

Rango de Puntaje	Descripción
[75- 100>	**Altamente Recomendable.** Cumple totalmente con los requerimientos y expectativas.
[50-74>	**Riesgoso**

Rango de Puntaje	Descripción
	Cumple parcialmente con los requerimientos, pero no se garantiza su adaptación a las necesidades.
[0-49>	No recomendable. Software con características inadecuadas.

7.5 Comparativo Técnico/Funcional

El siguiente cuadro describe el resultado de la evaluación por cada alternativa, agrupada desde el punto de vista del modelo de calidad sugerido por la Oficina Nacional de Gobierno Electrónico de la PCM.

El

Modelo/Característica/Sub Características		Alternativas			
		Kaspersky EndPoint Security Business - Advanced	Symantec Endpoint Protection Suite	Tren Micro Security	Intel Security
Calidad Interna y Externa					
Funcionalidad	Interoperabilidad	19	16	20	17
	Seguridad	25	21	25	19
	Adecuación	5	4	5	5
	Exactitud	5	3	5	3
Usabilidad	Entendimiento	4	4	5	3
	Operabilidad	10	8	10	8
Fiabilidad	Tolerancia a errores	5	3	5	5
Capacidad de Mantenimiento	Cambiabilidad	5	3	5	4
Portabilidad	Facilidad de instalación	5	4	5	14
	Reemplazabilidad	5	4	5	5
Calidad de Uso					
Satisfacción		5	4	5	5
Seguridad		5	3	5	5
Total		98	77	100	93

detalle de la evaluación por cada funcionalidad se describe en el **Anexo 3.**

8 ANÁLISIS COMPARATIVO COSTO - BENEFICIO

Costos referenciales de licencias, actualización, soporte y mantenimiento por 1 año.

ID	Software	Licencias	Fabricante	Precio Referencial (S/.)
1	Kaspersky EndPoint Security Business - Advanced	Sí	Kaspersky	S/. 192.79
2	Symantec Endpoint Protection Suite	Sí	Symantec	S/.101.96
3	Trend Micro Security	Sí	Trend Micro	S/.169.83
4	Intel Security (antes McAfee)	Sí	Intel Security	S/.125.00

Nota: El costo aproximado es referencial del mercado local y fue obtenida desde ofertas publicadas en Internet. Se precisa que es potestad de la Unidad de Logística, realizar el estudio de mercado, según la normatividad vigente.

Oficina de Tecnología de Información - V°B° IN Y GOB. - OGA - MTC

SERVICIOS TI - Informática - OTI - OGA - MTC

Fuente:

http://www.mejor-antivirus.es/analisis/comparativa-suites-de-seguridad-total.html

http://store.kaspersky.com/store/kasperla/custom/es_AR/pbPage.DR_LP_pe20branded?affiliate=drppc_gbs_DR_LP_pe20branded&ksid=2528e6df-a9ca-4a02-9f99-a156d8857ff6&ksprof_id=36&ksdevice=c&ksaffcode=583410&gclid=CKuU8pW8otICFRgHhgodXTAQPA

https://promos.mcafee.com/offer.aspx?id=1169502&gclid=COvGlJW9otICFVFbhgodTfwFVQ

http://www.trendmicro.es/productos/antivirus-plus-security/

OFICINA DE TECNOLOGÍA DE INFORMACIÓN - DIRECTOR

9. CONCLUSIONES

De evaluación técnico funcional de las herramientas de software de antivirus evaluadas, se determina que los software de seguridad antivirus N° 1 y 3, cumplen con los requisitos técnicos mínimos requeridos por la OTI.

Se recomienda la provisión de licencias de uno de los software en conformidad al informe de evaluación presentado con el objeto de proteger la información ante la amenaza de programas con código malicioso, virus, spyware, malware, etc.

10. FIRMAS

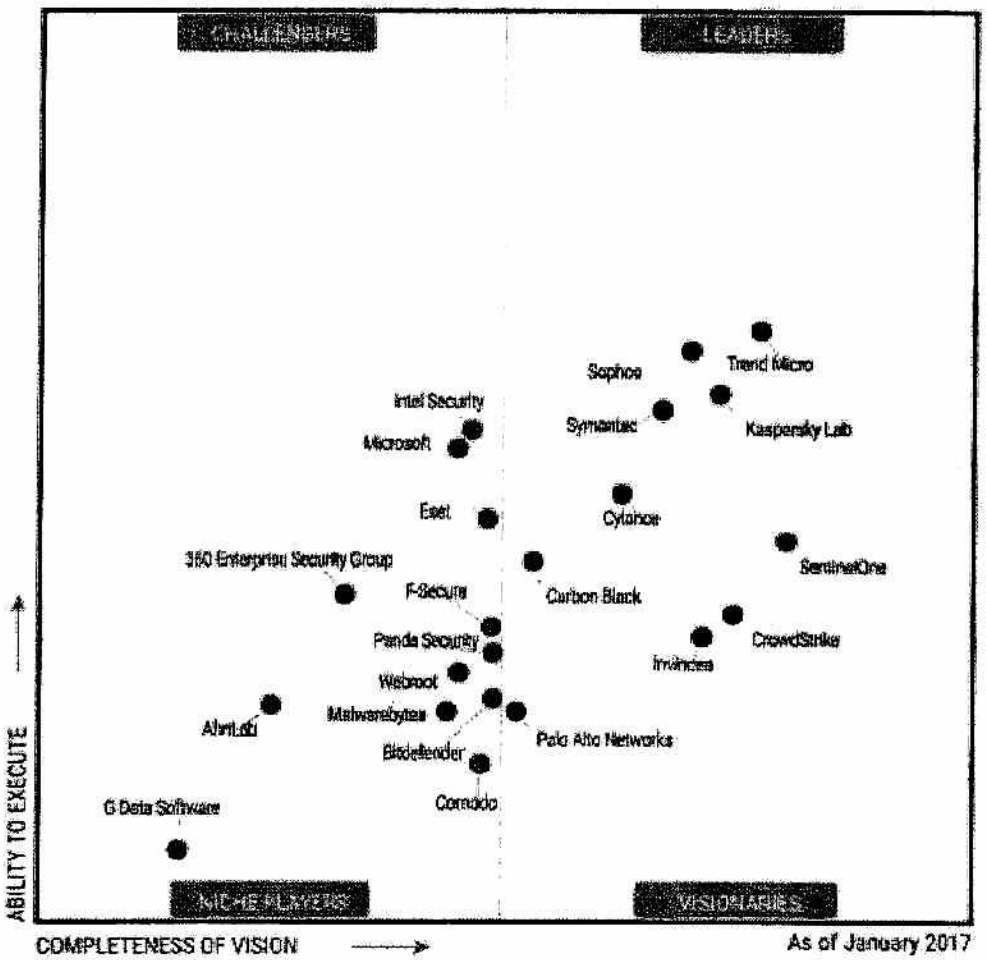
Patrick Manante Loayza
Analista de Seguridad Informática
Oficina de Tecnología de Información

Luis Roberto Blas Sernaque
Especialista normativo y regulación de TI
Oficina de Tecnología de Información

ROBERTO PUYÓ VALLADARES
DIRECTOR
Oficina de Tecnología de Información

ANEXO 1: CUADRANTE DE GARTNER[1]

Figure 1. Magic Quadrant for Endpoint Protection Platforms



SERVICIOS TI V°B° Seg. Informática OTI - OGA - MTC

Oficina de Tecnología de Información V°B° SERVICIOS OGA - MTC

OFICINA DE TECNOLOGÍA DE INFORMACIÓN V°B° DIRECTOR

[1] Gartner Inc. es una empresa consultora y de investigación de las tecnologías de la información a nivel mundial.

ANEXO 2: ATRIBUTOS DE EVALUACION DE SOFTWARE

2.1 TABLA RESUMEN DE PUNTAJES MÁXIMOS POR CARACTERISTICAS

Características	Puntaje Máximo
	100
Calidad Interna y Externa	**90**
Funcionalidad	55
Usabilidad	15
Fiabilidad	5
Capacidad de mantenimiento	5
Portabilidad	10
Calidad de Uso	**10**
Eficacia	5
Satisfacción	5

SERVICIOS TI - Informática - OTI - OGA - MTC

Oficina de Tecnología de Información - SERVICIOS - OGA - MTC

OFICINA DE TECNOLOGÍA DE INFORMACIÓN - DIRECTOR

2.2 TABLA DETALLADA DE PUNTAJES MÁXIMOS POR CARACTERISTICAS/SUB-CARACTERISTICAS

CALIDAD INTERNA Y EXTERNA PUNTAJE MAXIMO: 90		
Característica	**Sub Característica**	**Puntaje Máximo**
Funcionalidad La capacidad del producto de software para proveer las funciones que satisfacen las necesidades explícitas e implícitas cuando el software se utiliza bajo condiciones Específicas. **Puntaje máximo: 55**	**Interoperabilidad** La capacidad del producto de software de interactuar con uno o más sistemas especificados. La interoperabilidad se utiliza en lugar de compatibilidad para evitar una posible ambigüedad con la reemplazabilidad.	**20**
	Seguridad La capacidad del producto de software para proteger la información y los datos de modo que las personas o los sistemas o autorizados no puedan leerlos o modificarlos, y a las personas o sistemas autorizados no se les niegue el acceso a ellos. La seguridad en un sentido amplio se define como característica de la calidad en uso, pues no se relaciona con el software solamente, sino con todo un sistema.	**25**
	Adecuación La capacidad del producto de software para proveer un adecuado conjunto de funciones para las tareas y objetivos especificados por el usuario.	5
	Exactitud La capacidad del producto de software para proveer los resultados o efectos acordados con un grado necesario de precisión.	5
Usabilidad La capacidad del producto de software de ser entendido, aprendido, usado y atractivo al usuario, cuando es utilizado bajo las condiciones especificadas. **Puntaje máximo: 15**	**Entendimiento** La capacidad del producto de software para permitir al usuario entender si el software es adecuado, y cómo puede ser utilizado para las tareas y las condiciones particulares de la aplicación.	5
	Operabilidad **La capacidad del producto de software para permitir al usuario operarlo y controlarlo.**	10
Fiabilidad La capacidad del producto de software para proveer un desempeño adecuado, de acuerdo a la cantidad de recursos utilizados y bajo las condiciones planteadas. Los recursos pueden incluir otros productos de software, la configuración de hardware y software del sistema, y materiales (Ej: Papel de impresión o diskettes). **Puntaje máximo: 5**	**Tolerancia a errores** La capacidad del producto de software para mantener un nivel especificado de funcionamiento en caso de errores del software o de incumplimiento de su interfaz especificada.	5
Capacidad de mantenimiento Capacidad del producto de software para ser modificado. Las modificaciones pueden incluir correcciones, mejoras o adaptación del software a cambios en el entorno, y especificaciones de requerimientos	**Cambiabilidad** La capacidad del software para permitir que una determinada modificación sea implementada.	5

SERVICIOS TI V°B° Informática OTI - OGA - MTC

Oficina de Tecnología de Información V°B° SERVICIOS TI OGA - MTC

OFICINA DE TECNOLOGÍA DE INFORMACIÓN V°B° DIRECTOR

funcionales.y software del sistema, y materiales (Ej: Papel de impresión o diskettes). **Puntaje máximo: 5**		
Portabilidad La capacidad del software para ser trasladado de un entorno a otro. El entorno puede incluir entornos organizacionales, de hardware o de software. **Puntaje máximo: 10**	**Facilidad de instalación** La capacidad del producto de software para ser instalado en un ambiente especificado.	5
	Reemplazabilidad La capacidad del producto de software para ser utilizado en lugar de otro producto de software, para el mismo propósito y en el mismo entorno.	5

CALIDAD DE USO PUNTAJE MAXIMO: 10	
Característica	**Puntaje Máximo**
Eficacia La capacidad del producto de software para permitir a los usuarios lograr las metas especificadas con exactitud e integridad, en un contexto especificado de uso. **Puntaje máximo: 5**	5
Satisfacción La satisfacción es la respuesta del usuario a la interacción con el producto, e incluye las actitudes hacia el uso del mismo. **Puntaje máximo: 5**	5

PUNTAJE TOTAL	
CALIDAD INTERNA Y EXTERNA	= 90 puntos
CALIDAD DE USO	= 10 puntos
TOTAL	= 100 puntos

SERVICIOS TI - Vº Bº Coordinación Informática - OTI - OGA - MTC

Oficina de Tecnología de Información - Vº Bº SERVICIOS - OGA - MTC

DIRECTOR - DIRECCIÓN DE TECNOLOGÍA DE INFORMACIÓN

ANEXO 3. EVALUACION DETALLADA DE LAS HERRAMIENTAS DE SOFTWARE

Característica [1]	Sub Categoría	Métrica	Puntaje Máx.	Alternativas			
				Kaspersky EndPoint Security Business - Advanced	Symantec Endpoint Protection Suite	Trend Micro Security	McAfee EndPoint Protection Advanced
CALIDAD INTERNOS Y EXTERNOS (PUNTAJE MÁXIMO: 90)							
Funcionalidad	Adecuación	Capacidad de integrar tareas programadas para crear exclusiones, búsquedas avanzadas, cambio de nivel heurístico de seguridad.	5	5	4	5	5
Sub Total Adecuación			**5**	**5**	**4**	**5**	**5**
Funcionalidad	Interoperabilidad	Permite configuraciones de bloqueo virus, troyanos, gusanos, adware, spyware y otros programas potencialmente no deseados que roban datos confidenciales y sabotean la productividad de los usuarios.	5	5	4	5	5
Funcionalidad	Interoperabilidad	Contar con una gestión centralizada que permitirá gestionar el estado de la solución y monitorear los equipos informáticos.	5	5	3	5	5
Funcionalidad	Interoperabilidad	Capacidad de bloquear puertos de comunicación para evitar la propagación de la infección.	5	5	5	5	4
Funcionalidad	Interoperabilidad	Manejar un sistema basado en distribución de firmas de malware desde la consola principal hacia las estaciones de trabajo.	5	4	4	5	3
Sub Total Interoperabilidad			**20**	**19**	**16**	**20**	**17**
Funcionalidad	Exactitud	Permite detectar proactivamente ataques de Día Cero antes que estos lleguen a afectar los equipos de cómputo.	5	5	3	5	3
Sub Total Exactitud			**5**	**5**	**3**	**5**	**3**
Funcionalidad	Seguridad	Capacidad de detectar, analizar y eliminar programas maliciosos como virus, spyware, troyanos, keyloggers, programas publicitarios, etc.	5	5	4	5	4

SERVICIOS Vº Bº Seg. Informática OTI - OGA - MTC

Oficina de Tecnología de Información V°B° SERVICIOS

OFICINA DE TECNOLOGÍA DE INFORMACIÓN V°B° DIRECTOR

Característica [1]	Sub Categoría	Métrica	Puntaje Máx.	Alternativas			
				Kaspersky EndPoint Security Business - Advanced	Symantec Endpoint Protection Suite	Trend Micro Security	McAfee EndPoint Protection Advanced
Funcionalidad	Seguridad	Seguridad proactiva en la web y en el servicio de correo electrónico.	5	5	4	5	4
Funcionalidad	Seguridad	Control de actualizaciones y distribución automática en los equipos informáticos gestionados a través de la consola.	5	5	3	5	5
Funcionalidad	Seguridad	Contar con un mecanismo para garantizar que los clientes tengan los servicios activos, últimos componentes, consistencia en configuraciones y escaneos ejecutados.	5	5	5	5	3
Funcionalidad	Seguridad	La protección para estaciones finales deberá estar no solo basada en detección de firmas, sino también en patrones de comportamientos, reputación de archivos y sitios web.	5	5	5	5	3
Sub Total Seguridad			**25**	**25**	**21**	**25**	**19**
Usabilidad	Entendimiento	Capacidad del software de advertir a los usuarios sobre los sitios web maliciosos antes de que naveguen por ellos.	5	4	4	5	3
Sub Total Entendimiento			**5**	**4**	**4**	**5**	**3**
Usabilidad	Operabilidad	La solución deberá permitir manejar niveles de uso del CPU cuando el usuario ejecuta un escaneo manual.	5	5	4	5	5
Usabilidad	Operabilidad	Desplegar notificaciones en los equipos de los usuarios cuando existe una violación en la política de seguridad	5	5	4	5	3
Sub Total Operabilidad			**10**	**10**	**8**	**10**	**8**
Fiabilidad	Tolerancia a errores	La consola de administración centralizada debe soportar actualizaciones desatendidas y remotas para descargar y desplegar las actualizaciones.	5	5	3	5	5
Sub Total Madurez			**5**	**5**	**3**	**5**	**5**

SERVICIOS TI - V°B° Asist. Informática - OTI - OGA - MTC

Oficina de Tecnología de Información - V°B° SERVICIOS TI - OGA - MTC

OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN - V°B° DIRECTOR

Característica [1]	Sub Categoría	Métrica	Puntaje Máx.	Alternativas			
				Kaspersky EndPoint Security Business - Advanced	Symantec Endpoint Protection Suite	Trend Micro Security	McAfee EndPoint Protection Advanced
Capacidad de Mantenimiento	Cambiabilidad	Capacidad del software de implementar actualizaciones de seguridad por nuevas variantes de virus o software malicioso.	5	5	3	5	4
Sub Total Conformidad de Facilidad de mantenimiento			**5**	**5**	**3**	**5**	**4**
Portabilidad	Facilidad de instalación	Capacidad de instalación en modo silencioso y sin necesidad de reiniciar la estación de trabajo o servidor.	5	5	4	5	5
Sub Total Facilidad de instalación			**5**	**5**	**4**	**5**	**5**
Portabilidad	Reemplazabilidad	Control de actualizaciones de manera incremental y automática desde la solución de seguridad.	5	5	4	5	5
Sub Total Reemplazabilidad			**5**	**5**	**4**	**5**	**5**
CALIDAD DE USO (PUNTAJE MÁXIMO: 10)							
Eficacia	Permite al usuario proteger su información y actuar de manera proactiva frente a las amenazas.		5	5	4	5	4
Sub Total Eficacia			**5**	**5**	**4**	**5**	**4**
Satisfacción	Dar un soporte que impulse al usuario la comunicación proactiva para la prevención de errores, riesgos y fallas.		5	5	3	5	3
Sub Total Satisfacción			**5**	**5**	**3**	**5**	**3**
PUNTAJE TOTAL			**100**	**98**	**77**	**100**	**86**

Puntaje de adecuación: (Nivel Alto: 5, Nivel Medio: 4, Nivel Bajo: 3)

SERVICIOS TI - V°B° Seg. Informatica - OTI - OGA - MTC

Oficina de Tecnologías de Información - V°B° SERVICIOS TI - OGA - MTC

OFICINA DE TECNOLOGÍA DE INFORMACIÓN - V°B° DIRECTOR