



INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE
N° 002 -2018-OGETIC-SG/MC

**"ADQUISICIÓN DE LICENCIAS DE SOFTWARE ANTIVIRUS PARA LOS EQUIPOS
INFORMÁTICOS DEL MINISTERIO DE CULTURA"**

1. NOMBRE DEL ÁREA:

Oficina de Informática y Telecomunicaciones.

2. RESPONSABLE(S) DE LA EVALUACIÓN:

Ing. Javier Alberto Pala Garcia.

Director de la Oficina de Informática y Telecomunicaciones

Ing. Paola Cuba de la Flor

Soporte Técnico de La Oficina de Informática y Telecomunicaciones.

3. CARGO:

Director de la Oficina de Informática y Telecomunicaciones.

4. FECHA

09 de mayo de 2018.

5. JUSTIFICACIÓN

De acuerdo al Decreto Supremo N° 076-2010-PCM, toda entidad pública está obligada a utilizar software licenciado ya sea procedente de autores publicadores o vendedores (Software Libre y Software Propietario).



El Ministerio de Cultura necesita contar con una solución que garantice la adecuada protección de la información almacenada en los equipos y de los sistemas informáticos de la institución, de ser alterada, eliminada o copiada sin previo conocimiento del usuario responsable mediante el empleo de programas no deseados como virus informáticos, troyanos, spywares y la serie de variantes de los mismos.

En base a las nuevas amenazas es necesario considerar funcionalidades específicas para mitigar los riesgos con que actúan software de código malicioso (malware). Por lo cual se requieren software de antivirus robustos por ser una institución de impacto nacional.



Cabe resaltar, que anteriormente el Ministerio de Cultura contaba con el software ESET endpoint security, que incluían licencias con soporte y actualización de los mecanismos de protección sólo hasta el 10 enero del año 2017.

Por ello, es crucial contar con una solución antivirus para la institución por el nivel de tráfico de información de la red interna y descentralizada.

Por lo expuesto y por el marco de la Ley 28612 "Ley que norma el uso, adquisición y adecuación del software en la Administración Pública" se procede a evaluar el software de Antivirus Corporativo.

6. ALTERNATIVAS DE LA SOLUCIÓN

Considerando los requerimientos del Ministerio de Cultura se ha buscado alternativas de software en el mercado local que cumpla con dichos requerimientos y exista soporte técnico local.

Es por ello, que la herramienta de software que sea seleccionada debe contener como mínimo las funcionalidades que permitan mayor protección a la información que se maneja en el Ministerio de Cultura.



"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año del Diálogo y la Reconciliación Nacional"

Por lo mencionado, se ha establecido parámetros en base a la experiencia y a las mejores prácticas en el Ministerio de Cultura, estableciendo criterios que fortalezcan la seguridad en las TI obteniendo disponibilidad, integridad y confidencialidad, como factores que conlleven a una mejor evaluación.

Para realizar este análisis comparativo técnico, se eligieron los siguientes productos:

- Eset.
- Kaspersky.
- F-Secure.

7. ANÁLISIS COMPARATIVO TÉCNICO

El análisis técnico ha sido realizado en conformidad con la metodología establecida en la "Guía Técnica sobre evaluación de software en la administración pública" (R.M. N° 139-2004-PCM) tal como se exige en el reglamento de la Ley 28612.

A continuación, se presenta las métricas para esta evaluación:

Ítem	Atributos		Descripción	Puntaje
1	Calidad interna y externa			80
1.1	Funcionalidad	Adecuación	Soporta Sistema Operativos de estaciones de trabajo en versiones de 32 y 64 bits de Microsoft Windows 7, 8 y 10.	3
		Exactitud	Debe proteger contra virus, troyanos, macrovirus, adware, spyware, gusanos, rootkits y todo tipo de programa malicioso (malware) incluyendo la protección contra ransomware.	10
		Interoperabilidad	Interacción con bases de datos SQL así como herramientas de Microsoft Office, navegadores de internet, integración con el Directorio Activo	5
		Funcionalidad mínima	La solución como mínimo debe contar con una primera exploración automática después de la instalación del programa, lo que permite asegurar que el equipo se encuentra protegido desde el comienzo. La solución como mínimo deberá proteger contra virus, troyanos, macro virus, adware, spyware, gusanos, rootkits y todo tipo de programa malicioso (malware) incluyendo la protección contra ransomware. Administración centralizada.	12
1.2	Fiabilidad	Seguridad	Capacidad para proteger información y datos. Proteger con contraseña la configuración del antivirus para que no sea alterada.	3
		Madurez	Deberá incluir la protección contra vulnerabilidades y alerta de actualizaciones de software centralizada.	4
1.3	Usabilidad	Tolerancia a errores	Deberá permitir la instalación y desinstalación remota del software en el Endpoint centralizadamente.	3
		Entendimiento	La solución deberá monitorear y bloquear cambios no autorizados en el endpoint como cambios en el sistema,	5



"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año del Diálogo y la Reconciliación Nacional"

			modificación de llaves en el registro o creación de archivos y carpetas en áreas no autorizadas del sistema operativo.	
		Aprendizaje	Capacitación en el medio local.	5
		Operabilidad	Acceso de fácil interpretación y/o visualización (menú de cabecera)	4
1.4	Eficiencia	Comportamiento de tiempos	Alto rendimiento para análisis y procesos (velocidad de procesamiento)	3
		Utilización de recursos	Reducir el uso de recursos como memoria, CPU, y espacio en disco en máquinas virtuales.	3
1.5	Mantenimiento	Actualización	Facilidad para migrar a versiones superiores. Actualización de firmas manuales, y automáticas. Capacidad de uso de repositorios distribuidos.	3
		Soporte	Servicio técnico local.	4
1.6	Portabilidad	Adaptabilidad	Soporte diversos Sistemas Operativos.	3
		Facilidad de instalación	Contar con asistente de instalación, facilidad para su reinstalación.	2
		Coexistencia	Convivencia con diferentes software, sin causar conflictos	4
		Reemplazabilidad	La solución debe permitirá incorporar un mecanismo de reportes que permita programar la creación y envío de reportes en formato PDF y HTML vía correo.	4
22	Calidad en uso		Descripción	20
1	Eficacia		Capacidad del alcanzar metas operativas/indicadores del usuario en contexto específico de uso	5
2	Seguridad		La solución como mínimo deberá permitir proteger la navegación de los usuarios a sitios de banco y sitios confiables que se definan mediante el protocolo HTTPS con la finalidad de evitar el phishing o robo de datos a los usuarios.	5
3	Satisfacción		Capacidad para cubrir requerimientos con total conformidad del usuario.	10
Total				100

El análisis técnico y calificación de las métricas realizado a las alternativas de software se muestra en el siguiente cuadro:

Cuadro N° 01 - Análisis Comparativo Técnico

Ítem	Atributos		Puntaje	Alternativas		
1	Atributos internos y externos		80	ESET	Kaspersky	F-Secure
1.1		Adecuación	3	3	3	3
	Funcionalidad	Exactitud	10	6	8	6



"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año del Diálogo y la Reconciliación Nacional"

		Interoperabilidad	5	3	5	5
		Funcionalidad mínima	12	9	11	11
		Seguridad	3	3	3	3
1.2	Fiabilidad	Madurez	4	3	4	3
		Tolerancia a errores	3	3	3	3
1.3	Usabilidad	Entendimiento	5	3	4	4
		Aprendizaje	5	3	3	3
		Operabilidad	4	3	3	3
1.4	Eficiencia	Comportamiento de tiempos	3	2	3	2
		Utilización de recursos	3	3	2	2
1.5	Mantenimiento	Actualización	3	3	3	3
		Soporte	4	4	4	4
1.6	Portabilidad	Adaptabilidad	3	3	3	3
		Facilidad de instalación	2	2	2	2
		Coexistencia	4	3	3	3
		Reemplazabilidad	4	3	4	4
22	Calidad en uso		80	62	71	67
	Eficacia		5	4	5	4
	Seguridad		5	5	5	5
	Satisfacción		10	8	9	9
	Total		100	79	90	85

En este análisis un peso de 80 %.

De esta manera, se han evaluado las características técnicas de los productos mencionados y servicios adicionales, haciéndose verificado que uno de ellos cubre nuestras necesidades.

8. ANÁLISIS COMPARATIVO DE COSTO – BENEFICIO

Para la elaboración del análisis de costo beneficio se ha tomado en cuenta los criterios solicitados en el punto 8, del Reglamento de la Ley N° 28612.

Cuadro N° 02 - ANÁLISIS COSTO-BENEFICIO

Nro.	Criterios a evaluar	ESET	Kaspersy	F-Secure
1	Licenciamiento.	Requerido	Requerido	Requerido
2	Licenciamiento x 1 año (precio Unitario)	S/. 139.00	S/. 14.85	S/. 249.00
3	Hardware necesario para su funcionamiento.	Si	Si	Si
4	Capacitación.	No	Si	No
	TOTAL (S/.)	S/. 139.00	S/. 133.85	S/. 249.00

Este análisis tiene un peso del 20%

Fórmula de cálculo de puntaje:

Puntaje de Menor costo (mc) = 100 ptos.

Puntaje de Mayor costo (MC) = (mc/MC) * 100

Link de los precios mostrados en el cuadro N° 2



"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año del Diálogo y la Reconciliación Nacional"

<https://pe.tienda.eset-la.com/eset-nod32-antivirus?gclid=Cj0KCQjwuMrXBRC ARIsALWZrlgagEpN5MZIYO147W73tKcy2RHdJ6YclFkkeqztz BLDgFM-9ADUcgaAsMVEALw wcB>
<https://www.kaspersky.com/antivirus>
https://promos.mcafee.com/offer.aspx?id=1338788&utm_source=google-nonbrand-c&utm_campaign=1165972943&utm_content=265868930108&utm_term=kwd-332968079660&gclid=Cj0KCQjwuMrXBRC ARIsALWZrljCVFNp2iUEMtopslEL1b8t8ox2p9h J-YNgtGpowccBq-PenrZlaAnAOEALw wcB

A continuación, se presente el siguiente cuadro, el resultado global del análisis técnico y el análisis costo beneficio:

Nro.	Criterios a evaluar	ESET	Kaspersy	F-Secure
1	Análisis Comparativo Técnico	63.2	72	68
2	Análisis Costo Beneficio	19.26	20	10.75
TOTAL		82.46	88.26	80.59

Cuadro N° 03 - RESUMEN DE EVALUACIÓN GLOBAL

9. CONCLUSIONES

La Oficina de Informática y Telecomunicaciones, tiene la necesidad de contar con nuevas licencias de software solución de antivirus.

Los costos de las licencias de las marcas evaluadas son variables, siendo las soluciones de software antivirus de las marcas: ESET, Kaspersky y F-Secure las evaluadas.

En conclusión, por los motivos ya señalados, se recomienda adquirir Software Antivirus de las marcas que obtuvieron un puntaje mayor a 80 puntos, ya sea ESET, Kaspersky y F-Secure, dado que las soluciones evaluadas cumplen con lo mínimo necesario, garantizará el adecuado funcionamiento de las estaciones y servidores de la entidad, ante cualquier ataque de Virus o Software malintencionado.

10. FIRMA

Responsable de la Evaluación	Firma
Ing. Paola Cuba de la Flor Soporte Técnico de La Oficina de Informática y Telecomunicaciones	
Responsable de la Aprobación	Firma
Ing. Javier Alberto Pala Garcia Oficina de Informática y Telecomunicaciones	