Tribunal Constitucional

Oficina de Tecnologías de la Información

Informe Técnico de Previo de Evaluación de Software

N° ITPES – 01 – 2021-OTI/TC

Software de protección antiviral

Julio 2021

Tribunal Constitucional

INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE N° 001-2020

SOFTWARE ANTIVIRUS

1. NOMBRE DEL ÁREA

Oficina de Tecnología de la Información

2. RESPONSABLE DE LA EVALUACION

Ing. Cesar Rodríguez Alegre

3. CARGO

Jefe de la Oficina Tecnología de la Información

4. FECHA

02/07/2021

5. JUSTIFICACION

Actualmente el Tribunal Constitucional cuenta con un Software Antivirus para los equipos de cómputo que operan tanto en sus sedes, como en aquellos que han sido distribuidos en razón al estado de emergencia, cuyo periodo de vigencia está próximo a vencer, el cual cumple de manera aceptable la protección de las estaciones de trabajo y servidores frente a amenazas de virus informáticos, troyano, spyware y otros tipos de malware. No obstante, la nueva normalidad de trabajo y las cada vez más constantes

Dado lo antes señalado y con el objetivo de proteger los equipos informáticos, salvaguardar la información y garantizar la operatividad y continuidad del servicio que brinda la institución, se requiere implementar una solución de software antivirus para los equipos informáticos del Tribunal Constitucional, que funcione con altos niveles de desempeño y que sean capaces de proteger a equipos que no necesariamente se encuentren dentro de los recintos institucionales, sino incluso a equipos conectados a Internet con distintos proveedores de acceso a Internet (ISP) y desde locaciones tanto nacionales como internacionales.

6. ALTERNATIVAS DE EVALUACION

El Tribunal Constitucional cuenta con aproximadamente equipos de cómputo entre computadoras personales, servidores y dispositivos móviles que necesitan ser protegidos de eventuales ataques informáticos. Considerando las necesidades mencionadas se ha buscado alternativas de software en el mercado local que cumplan con el perfil de requerimientos necesarios y con el respectivo soporte técnico local.

Es por ello que la herramienta de software que se vaya a seleccionar, consecuencia del presente proceso evaluativo debe contener como mínimo las funcionalidades que permitan disponer de los mayores niveles de protección de la información.

Por consiguiente, se ha establecido parámetros mínimos que permitan fortalecer 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:

- Kaspersky
- Sophos
- Comodo Antivirus

La razón por la que se ha elegido como programas sujetos a evaluación consiste en que los dos primeros ya han sido utilizados con anterioridad por la institución, en tanto que el tercero es un programa que ha sido evaluado debido a que es el que más se asemeja a los programas anteriormente utilizados y la familiarización del personal técnico con las funcionalidades que ofrece este producto resulta similar a los otros dos productos.

7. ANALISIS COMPARATIVO TECNICO

El análisis se ha realizado en conformidad con la metodología establecida en la "Guía Técnica sobre evaluación de software en la administración pública"[1] tal como lo recomienda el reglamento de la Ley 28612[2].

A continuación, se presenta las métricas para esta evaluación.

Modelo de calidad para la calidad Interna y Externa

Características y Atributos Internos y Externos			Puntaje Máximo
Característica	**Atributos**	**Descripción del atributo**	
Funcionalidad	Adecuación	Soporte a Sistema Operativo Windows : Para estaciones de trabajo Windows 7/8/10. Para servidores: Windows 2008/2012/2012R2/2016 server. En ambos casos para S.O. de 32 y 64 bits Otros sistemas operativo no windows: Linux (CentOs, Oracle Linux, MacOs)	3

[1] Aprobada mediante R.M. N° 139-2004-PCM

[2] Aprobada mediante D.S. Nº 024-2005-PCM

	Exactitud	El sistema de antivirus deberá detectar y eliminar en tiempo real, virus, gusanos, troyanos, macrovirus, keyloggers, dialers, adware, spyware, hacktools, rootkits, bots, ransomware y otros programas potencialmente peligrosos en todos los archivos residentes en memoria, comprimidos (cualquier formato de compresión, rar, zip, cab, arj, arz) en no menos de 50 niveles, ocultos y archivos de ejecución. El sistema de antivirus deberá contar con una tecnología Heurística propia avanzada que elimine al malware basado en su comportamiento malicioso en tres niveles (bajo, medio y alto) y no basándose en listas de vacunas de virus o en firmas de virus.	3
	Interoperabilidad	Interacción con bases de datos SQL, así como herramientas de Microsoft Office, navegadores de internet, integración con el Directorio Activo. El sistema de antivirus deberá ser capaz de revisar los macros de los documentos de office para de esta manera detectar actividad ilícita por parte de algún tipo de malware	4
	Seguridad	El sistema de antivirus deberá contar con una herramienta de detección que elimine los malware por comportamiento a través de su propia heurística y no basada en una lista de firmas de virus convencionales.	4

	Conformidad de Funcionabilidad	La solución de antivirus como mínimo deberá contar con una primera exploración automática después de la instalación del programa, lo que permite asegurar que el equipo se encuentre protegido desde el comienzo. La solución como mínimo deberá proteger contra amenazas: virus, gusanos, troyanos, keyloggers, dialers, adware, spyware, hacktools, rootkits, bots, phishing, herramientas de control remoto y todo tipo de programa malicioso (malware) incluyendo la protección contra ransomware. Disponer de Consola de Administración.	4
Seguridad	Madurez	Deberá incluir la protección contra Vulnerabilidades y alertas de Actualizaciones de software centralizado	4
	Tolerancia a fallas	Deberá permitir la instalación y desinstalación remota del software en el EndPoint centralizadamente	4
	Recuperabilidad	Debe contar con un sistema de contención (Sandbox) que respalde exclusivamente al sistema de antivirus con el fin de evitar y prevenir las infecciones de malware que el motor de antivirus no llegue a detectar. Esta herramienta debe funcionar como una segunda capa de seguridad que permita ser instalado en cada PC y servidor	4
	Conformidad de Fiabilidad	Debe permitir analizar archivos desconocidos en línea con un rango de verificaciones estáticas y de comportamiento en tiempo real que permita identificar aquellos archivos que son maliciosos	4
Usabilidad	Entendimiento	La consola de administración central deberá permitir la administración simultánea de equipos, servidores y dispositivos móviles bajo sistemas operativos Windows, Linux, Mac IOS y Android.	4

	Aprendizaje	La consola de administración central deberá encontrarse en la nube. Esta consola deberá permitir administrar desde un solo punto todas las oficinas y redes de la institución	3
	Operabilidad	La consola de administración central deberá ser escalable, lo cual permitirá activar la administración de redes complejas, permitiendo la administración de todos los equipos con que cuenta el Tribunal	4
Eficiencia	Comportamientos de tiempos	Alto rendimiento para análisis y procesos (velocidad de procesamiento)	4
	Uso de recursos	El sistema de contención deberá contar con un entorno virtual donde las nuevas amenazas de malware que el antivirus no detecta y deja sean contenidas y bloqueadas a nivel de red para impedir cualquier tipo de propagación e infección.	4
Capacidad de Mantenimiento	Capacidad de ser actualizado	Debe contar con una herramienta de veredicto en la nube que analice cada archivo según su comportamiento y genere una actualización heurística actualizable con el motor de antivirus con una respuesta máximo de 3 minutos permitiendo eliminar la nueva amenaza.	4
	Cambiabilidad	La plataforma de mesa de ayuda (Service Desk) debe permitir a los administradores y al personal de soporte realizar un seguimiento y responder a los tickets generados por los usuarios. La plataforma de mesa de ayuda debe permitir reasignar tickets a cada técnico de forma automática o personalizada siempre que estos no cuenten con el tiempo requerido para dicho soporte.	4

	Estabilidad	Debe integrar un firewall cliente para el control del tráfico de red LAN que permita ser instalado en cada PC, un sistema de alcance antiviral que proteja a los procesos activos ante los ataques de bots y rootkits; que permita ser instalado en cada PC y servidor, un sistema HIPS para prevenir la intrusión de hacking, anti-proxy, hackers y spyware que permita ser instalado en cada PC y servidor.	4
	Facilidad de prueba		4
	Conformidad de facilidad de mantenimiento	El sistema de contención deberá permitir dar privilegios al administrador de la red en decidir liberar o bloquear aplicativos que considere buenos o malos para su entorno de seguridad en la red. El sistema de contención deberá ser administrado desde una consola de administración central.	4
Portabilidad	Facilidad de Instalación	El sistema de administración de TI deberá contar con una herramienta que permita bloquear dispositivos ejemplos: Lector de CD y DVD, USB, inflarrojo, buetooth, card reader, lector de floppy, medios de almacenamiento por conexión USB, por ejemplo: HDD externos, USB pendrive, almacenamiento de celulares Android, Iphone, Tablet, memorias SD entre otros esta política debe ser reflejada y administrada a través de la consola de administración centralizada	3
	Coexistencia	La consola centralizada de tener la capacidad de operar en la nube	4
Sub total Modelo de Calidad para la Calidad Interna y Externa			80

Tribunal Constitucional

Modelo de calidad para la calidad de uso

Características y Atributos Internos y Externos		Puntaje Máximo
Atributo	**Descripción de la atributo**	**20**
Eficacia	Entendido como la capacidad de producto de cumplir con el objetivo primario, cual es la protección del equipo de cómputo y la red en su conjunto del ataque de cualquier amenaza del tipo malware (virus informáticos y todas las diferentes variantes de ellos)	5
Productividad	La solución como mínimo deberá proteger todos los procesos habituales que se lleven a cabo en el equipo, entre ellos: la navegación en Internet, apertura de correos electrónicos, ejecución de archivos, análisis de archivos empaquetados, ejecución de macros etc.	5
Satisfacción	Entendida como la capacidad satisfacer los requerimientos tanto del usuario final como el administrados de la red y del panel de control	5
Seguridad	Entendido como la capacidad del producto que su uso resulte segura para el equipo sobre el que es instalado y que a su vez de cumplir con la finalidad para que el que es adquirido, no provoque algún daño colateral como consecuencia de su uso	5
Sub total Modelo de Calidad para la Calidad de uso		**20**

Tribunal Constitucional

Análisis Comparativo y calificación en razón al modelo de Calidad

Análisis Comparativo Técnico

A. Para el Modelo de Calidad para la Calidad Externa e Interna

Características y Atributos Internos y Externos		Puntaje	Alternativas		
Característica	**Atributos**	**80**	**Kaspersky**	**Sophos**	**Comodo**
Funcionalidad	Adecuación	3	3	3	3
	Exactitud	3	3	3	3
	Interoperabilidad	4	3	3	4
	Seguridad	4	3	3	4
Seguridad	Madurez	4	3	3	4
	Tolerancia a fallas	4	3	4	1
	Recuperabilidad	4	3	3	4
	Conformidad de Fiabilidad	4	4	4	4
Usabilidad	Entendimiento	4	4	4	4
	Aprendizaje	3	2	2	3
	Operabilidad	4	3	3	4
Eficiencia	Comportamientos de tiempos	4	4	4	3
	Uso de recursos	4	3	3	3
Capacidad de Mantenimiento	Capacidad de ser actualizado	4	3	3	4
	Cambiabilidad	4	3	3	4
	Estabilidad	4	3	3	4
	Facilidad de prueba	4	4	4	4
	Conformidad de facilidad de mantenimiento	4	3	4	4
Portabilidad	Facilidad de Instalación	3	3	3	3
	Coexistencia	4	3	3	4
Sub total Modelo de Calidad para la Calidad Interna y Externa		**80**	**67**	**69**	**75**

B. Para el Modelo de Calidad para la Calidad de Uso

Atributo	Puntaje	Alternativas		
	20	**Kaspersky**	**Sophos**	**Comodo**
Eficacia	5	5	5	5
Productividad	5	5	5	5
Satisfacción	5	5	5	5
Seguridad	5	5	5	5
Sub total Modelo de Calidad para la Calidad de uso	**20**	**20**	**20**	**20**

Puntuación Total para el Modelo de Calidad	**100**	**87**	**89**	**95**

8. ANALISIS COMPARATIVO COSTO-BENEFICIO

Para la elaboración del análisis de costo beneficio se ha tomado en cuenta los criterios planteados en el punto 8, del Anexo I del reglamento de la Ley N° 28612 sobre Requisitos mínimos del Informe Técnico Previo de Evaluación de Software

Con el objetivo de otorgar mayor objetividad en el proceso de evaluación del costo monetario, se ha optado por otorgar el puntaje de 100 al menor costo y penalizar a los de precios más elevados, de la siguiente manera:

$$\text{Penalidad} = \frac{\text{Costo de Opción - Costo de Opción más económica}}{\text{Costo de Opción más económica}}$$

El puntaje para cada opción se obtendrá de restar de 100 la penalidad calculada.

De este modo se obtiene el siguiente cuadro:

ANALISIS COMPARATIVO DE COSTO - BENEFICIO

Conceptos	Productos Evaluados Puntaje obtenido		
	Kaspersky[1]	Sophos[2]	Comodo[3]
Implementación, soporte técnico y Licencia con vigencia de 24 meses	36,820.00	62,410.20	41,300.00
Penalización	0.00	69.50	12.17
Puntaje	100.00	30.50	87.83

[1] El precio referencial para el costo asignado a la opción Kaspersky se ha tomado de la Orden de Servicios 0000127-2018 del 19/07/2018, en el que se compraron 250 licencias, desde lo cual se ha proyectado el precio para 350 licencias, por dos años

[2] El precio referencial para el costo asignado a la opción Sophos se ha tomado de la Orden de Servicios 0000073-2020 del 17/08/2020, en el que se compraron 350 licencias, por un año. Se ha proyectado para una adquisición por dos años

[3] El precio referencial para el costo asignado a la opción Comodo se ha tomado de una cotización planteada por un distribuidor del producto sobre la base de 350 licencias, por un año. Se ha proyectado para una adquisición por dos años

Para el análisis final se otorgará un peso de 80% a la evaluación técnica y un peso de 20% a la evaluación de Costo-Beneficio, con lo que se obtiene el siguiente cuadro.

Tribunal Constitucional

Cuadro Resumen de Evaluación Comparativa

Tipo de Análisis	Peso otorgado	Alternativas		
		Kaspersky	Sophos	Comodo
Comparativo Técnico	80%	69.60	71.20	78.40
Comparativo Costo Beneficio	20%	20.00	6.10	17.57
Calificación Final	**100%**	**89.60**	**77.30**	**95.97**

Los cuadros anteriores muestran la evaluación de las características tanto técnicas como económicas de los productos materia de la evaluación.

9. CONCLUSION

Después de haber realizado las evaluaciones recomendadas por la normatividad vigente se concluye que la mejor opción que satisface técnica y económicamente las necesidades de protección antiviral es la que ofrece el producto denominado Comodo Antivirus, por lo que se recomienda plantear los términos de referencia que permitan su adquisición.

10. FIRMA DEL RESPONSABLE DE LA EVALUACIÓN.