INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE N° 001- 2021-MML-IMP-OGIT

SUSTENTO TÉCNICO PARA LA ADQUISICIÓN DE SOFTWARE ANTIVIRUS Y ANTIMALWARE CORPORATIVO

1. **NOMBRE DE ÁREA:**
   Oficina General de Información Técnica

2. **RESPONSABLE DE EVALUACIÓN:**
   Ing. Daniel Romero Delgado

3. **CARGO:**
   Director General de Jefe de la Oficina General de Información Técnica

4. **FECHA:**
   24 de febrero de 2021

5. **JUSTIFICACIÓN:**
   El Instituto Metropolitano de Planificación (IMP) de la Municipalidad Metropolitana de Lima, necesita contar con una solución que garantice la adecuada protección de la información que se comparte, 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, spyware, software malicioso 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 el software de código malicioso. Por lo cual se requiere adquirir un Software Antivirus y Antimalware Corporativo robusto por ser una institución de impacto nacional. Por ello, es crucial contar con un Software Antivirus y Antimalware Corporativo para el IMP con el fin de asegurar el tráfico de información en las Redes LAN y WAN. Por lo expuesto y el marco de Ley 28612 "Ley que norma el uso, adquisición y adecuación del software en la Administración Publica" se procede a evaluar el Software Antivirus y Antimalware Corporativo.

6. **ALTERNATIVAS:**
   Considerando los requerimientos del IMP 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 minino con las funcionalidades que permitan mayor protección a la información que se maneje en el IMP.

   Para realizar este análisis comparativo técnico, se eligieron los siguientes tres (03) productos reconocidos en el Cuadrante Mágico de Gartner ya sea como Líderes o Visionarios y que tuvieran por lo menos un representante autorizado en el Perú.

Las alternativas seleccionadas se muestran a continuación:

SOFTWARE ANTIVIRUS Y ANTIMALWARE CORPORATIVO	F-Secure Business Suite Premium
	Sophos Intercept X Avanzado
	Kaspersky Total Security for Business

Para la evaluación, se ha establecido parámetros en base a los requerimientos de seguridad antivirus de la institución, la experiencia y a las mejores prácticas en el IMP, obteniendo disponibilidad, integridad y confidencialidad, como factores que conlleven a una mejor evaluación.

La evaluación se hará realizando los parámetros establecidos en la RM 139-2004-PCM "Guía Técnica sobre Evaluación de Software en la Administración Pública".

7. **ANALISIS COMPARATIVO TÉCNICO:**
Las métricas fueron identificadas de acuerdo a los criterios de las especificaciones técnicas del IMP.

Cuadro de Comparaciones de Métricas: Ver Anexo 01

8. **ANALISIS COMPARATIVO DE COSTO – BENEFICIO:**
No aplica. Dado que este punto deberá ser reflejado con el estudio de mercado.

9. **CONCLUSIONES:**
El IMP tiene la necesidad de contar con las licencias de software antivirus y antimalware corporativo, dado que la solución actual esta pronto a caducar. Los costos de las licencias de las marcas evaluadas son variables, siendo las soluciones de software antivirus de las marcas: F-Secure Business Suite Premium, Kaspersky Total Security for Business las que presentan mayores ventajas técnicas. En conclusión, por los motivos señalados, el Software Antivirus y Antimalware Corporativo que obtuvieron un puntaje mayor a 140 puntos son Kaspersky Endpoint o F-Secure Business, los cuales permitirán contar con un adecuado funcionamiento de las estaciones y servidores de la entidad ante un ataque de Virus o Software malintencionado. Así mismo, el producto Sophos InterceptX ha obtenido un menor puntaje debido a que la marca no tiene un producto que se instale on-premise en su última versión

IMP INSTITUTO METROPOLITANO DE PLANIFICACIÓN
MUNICIPALIDAD METROPOLITANA DE LIMA

Ing. Daniel Romero Delgado
Director General de la
Ofic. General de Información Técnica (e)

ANEXO 01

N°	Métricas	Descripción	Puntaje Máximo	F-Secure Business Suite Premium	Sophos Intercept X Avanzado	Kaspersky Total Security for Business
Métricas Internas						
1	Sistemas Operativos Soportados	Para estaciones de trabajo: Microsoft Windows Vista, 7, 8, 8.1, 10. Para servidores Windows Server: 2008 R2, 2012, R2 y Linux.	10	10	10	10
2	Protección	Debe tener instalado los siguientes componentes: Antivirus, antispyware, firewall, control web, antispam, IDS o HIPS y control de dispositivos extraibles y antiransomware.	10	10	10	10
3	Antivirus	Debe tener la capacidad de analizar, estudiar y reconocer el comportamiento de los códigos maliciosos (malware). Debe tener un módulo de revisión de antivirus residente, ejecutándose sistemas operativos y un módulo de revisión antivirus de forma manual por el usuario. Deberá contar con tecnología que evite que los códigos maliciosos desactiven componentes del sistema.	10	10	10	10
4	Administración	Diseñada para trabajar en ambiente de red, con administración centralizada oo-premise.	10	10	S	10
5	Sestión de Sarches y /ulnerabilidades	Debe analizar y reconocer las vulnerabilidades existentes y nuevas, asi como poder descargar y aplicar las correcciones de estos en forma centralizada y utilizando mecanismos de optimización de uso de ancho de banda.	10	10	S	8
6	Consola	Debe permitir la gestión, monitoreo y administración de los equipos con el agente antivirus instalado que se encuentra en la red LAN. WAN y equipos con conexiones a internet. Debe permitir recibir y generar reportes de los equipos que cuenten con el agente de antivirus instalado. Tener la capacidad de cambiar la configuración de múltiples clientes a la vez sin la intervención del usuario final. La consola deberá realizar búsquedas de estaciones de trabajo y/o servidores. La consola se puede instalar tanto en la nube como on- premise en sus últimas versiones.	10	10	S	8
Métricas Externas						
1	Eficacia	Debe tener la capacidad de reconocer el mafware que no se encuentre en su base de datos, mediante el uso de un sistema de heurística avanzada.	10	10	10	10
2	Actualización de firmas	Las actualizaciones de firmas y componentes del antivirus deberán ejecutarse de manera centralizada, desatendida e incremental.	10	10	10	10
3	Control de dispositivos	El software de antivirus deberá permitir el acceso de solo lectura, lectura/escritura o bloquear dispositivos, como: USB, CD-ROM y discos externos entre otros.	10	10	9	10
4	Idioma	Su interfaz debe encontrarse en español.	10	10	10	10
5	Alertas	Deberá de generar alertas ante un evento especifico mediante el envío de mensajes de correo o notificaciones vía SNMP.	10	10	10	10
Métricas de Uso						
1	Facilidad de uso e instalación	El uso de interface debe ser fácil, amigable e intuitiva.	10	9	9	7
2	Generación de alertas y reportes	Se podrán generar una amplia variedad de reportes predefinidos o personalizados y presentar alertas en las PCs y consola. Los reportes podrán ser obtenidos de forma automática o a intervalos de tiempo predefinidos.	10	10	10	10
3	Soporte Local	Cuenta con un representante local, que brindará el soporte respectivo cuando se requiera.	10	10	10	10
4	Manejo de consola administrativa	La interface de consola debe ser amigable e intuitiva.	10	9	9	8
		Total	**150**	**148**	**132**	**141**

INSTITUTO METROPOLITANO DE PLANIFICACIÓN
Municipalidad Metropolitana de Lima
Ing° DANIEL ROMERO DELGADO
IMP