INFORME TÉCNICO PREVIO DE EVALUACION DE SOFTWARE N° 002-2018-GR.CAJ/GRPPAT/CIS-RJAI

"SUSTENTO TÉCNICO PARA LA ADQUISICIÓN DE LICENCIAS DE SOFTWARE ANTIVIRUS"

GOBIERNO REGIONAL Cajamarca
EXPEDIENTE
N° 3678499

1. **Nombre del Área**

   Centro de Información y Sistemas

2. **Responsable de la Evaluación**

   Reinaldo Javier Aliaga Infante

3. **Cargo**

   Ingeniero de Sistemas II – Administrador de Redes y Servidores

4. **Fecha**

   14 de marzo de 2018

5. **Justificación**

   Cumpliendo con la Norma Técnica Peruana NTP ISO/IEC 27001:2014 EDI. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información, el Gobierno Regional de Cajamarca cuenta con 600 licencias de Kaspersky Total Security for Business. Dicho software ayuda a mitigar riesgos de infección de todos los equipos de cómputo contra virus y malware.

   Las licencias en mención, tienen una vigencia de tres años, esa vigencia culmina el 30 de junio del 2018, es por ello que se requiere adquirir una solución de seguridad para proteger computadoras de escritorio, computadoras portátiles y servidores de la Sede Central y Unidades rindentes del Gobierno Regional de Cajamarca ante los riesgos ya mencionados en el párrafo anterior.

6. **Alternativas de Evaluación**

   Para el análisis se ha seleccionado los siguientes softwares ofimáticos:

   - Kaspersky Total Security for Business
   - Symantec Endpoint Protection
   - ESET Endpoint Security

7. **Análisis comparativo Técnico**

   Para este fin se aplicará el modelo de calidad externa interna y se han considerado los siguientes atributos como relevantes para el análisis técnico:

NRO	ATRIBUTO	DESCRIPCIÓN DE ATRIBUTO
ATRIBUTOS INTERNOS		
1	Modalidad de actualizaciones	Ejecución desatendida e incremental, y manual de actualización de firmas y componentes
2	Protección en tiempo real	Proporcionar protección en tiempo real mediante niveles predefinidos de protección o personalizado por el usuario de acuerdo a sus requerimientos. El módulo de detección en tiempo real debe proteger contra: virus, gusanos, troyanos, keyloggers, dialers, adware, spyware, hacktools, rootkits, bots, spam, malware, herramientas de control remoto y otros programas potencialmente peligrosos.
3	Soporte a sistemas operativos cliente	Windows 7 o Superior, Mac OS, Linux (32 y 64 bits)
4	Soporte a sistemas operativos servidor	Windows Server 2012 o Superior Linux CentOS 7 o superior de 32 y 64 bits según corresponda.
5	Soporte a dispositivos móviles	Compatible con las plataformas móviles más populares.
6	Protección contra amenazas de día cero	El fabricante de la solución deberá ofrecer protección contra amenazas de día cero. Las firmas deben estar basada en patrones que ayuden a mejorar las tasas de detección de malware y reduzcan el tamaño de las actualizaciones de la base de datos, para mejorar la seguridad y reducir la carga en la red.
7	Protección Proactiva en el host	La solución antivirus deberá monitorear automáticamente cómo se comportan las aplicaciones cuando se ejecutan en sus sistemas. Si detecta un comportamiento sospechoso, la solución deberá bloquear la aplicación.
8	Protección Proactiva en la red	Contar con tecnología que detecte actividades sospechosas en una red corporativa y que las monitorea. Además, de pre configurar cómo los sistemas responderán en caso de que se identifique un comportamiento sospechoso

9	Sistema de Prevención de Intrusos	Contar con un sistema de prevención de intrusiones basado en host y un firewall personal que brindan un control flexible sobre el tráfico de entrada y salida. Puede establecer parámetros para puertos, direcciones IP o aplicaciones específicos.
10	Escaneos Personalizados	Escaneos manuales o programados, indicándose las unidades a escanear o las carpetas específicas que requieren ser escaneadas
11	Protección por contraseña	El producto debe pedir una contraseña ante intentos de cambio indebidos en su configuración.
12	Componentes de la Solución	El producto debe contar con un cliente antivirus y con un agente que le permita ser administrado desde una consola centralizada.
13	Antispam a nivel de cliente	La solución antivirus debe ser capaz de revisar spam cliente a nivel de los protocolos POP3, SMTP, IMAP.
14	Control Web	Monitoreo y filtrar el uso del navegador web de cada empleado. Permitir, prohibir, limitar o auditar el acceso de los usuarios a sitios web o categorías de sitios web específicos, como sitios de juegos, de apuestas o de redes sociales.
15	Control de Dispositivos	Herramientas de control de dispositivos para la administración de dispositivos extraíbles (USB, CD-ROM) y proteger contra los riesgos de seguridad que pueden añadir los dispositivos no autorizados. La solución debe permitir: Administrar privilegios de acceso para un tipo específico de dispositivo, un bus o un dispositivo individual (según su número de serie único). Pre configurar los momentos en que se aplican sus políticas de control de dispositivos, tales como evitar el uso de dispositivos fuera de los horarios de oficina normales
16	Motor Heurístico	Motor heurístico para detección de posibles nuevos virus, el nivel de la heurística debe poder ser personalizable. La solución antivirus debe combinar tecnologías antimalware basadas en firmas, en el análisis heurístico y en los servicios de nube, para brindar protección contra amenazas conocidas y emergentes.

17	Cifrado	Debe permitir elegir entre el nivel de disco completo o el de archivo, respaldado por el algoritmo Advanced Encryption Standard (AES), con cifrado de 256 bits, permitiendo proteger información empresarial de vital importancia en caso de robo o pérdida de dispositivos.
18	Cifrado - Compatibilidad con dispositivos extraíbles	Aumenta la seguridad mediante políticas que aplican el cifrado de datos en dispositivos extraíbles
19	Cifrado - Uso compartido de datos seguros	La solución debe permitir a los usuarios crear fácilmente paquetes cifrados y autoextraíbles para garantizar que los datos estén protegidos al compartirlos mediante dispositivos extraíbles, correo electrónico, redes o la web
20	Cifrado - Transparencia para usuarios finales	La solución de cifrado debe ser invisible para los usuarios y no deberá tener efectos negativos en la productividad. Sin repercusiones en la configuración de las aplicaciones ni en las actualizaciones
21	Protección de Correo Corporativo Múltiples plataformas	Protección de múltiples plataformas, compatible con una amplia gama de servidores de correo, incluidos Microsoft Exchange, IBM Lotus Notes/Domino, Sendmail, qmail, Postfix.
22	Protección de Correo Corporativo - Filtrado	Filtrado de spam
23	Protección de Correo Corporativo - Protocolos	Protección del tráfico, mediante protección al tráfico que circula por las puertas de enlace más populares basadas en Windows o Linux, pues eliminan de manera automática los programas potencialmente hostiles y maliciosos que aparecen en el tráfico HTTP(S), FTP, SMTP y POP3
24	Consola de Administración	La solución antivirus debe poseer una consola de administración centralizada a la cual pueda reportar el estado de todos los equipos conectados a la red corporativa.
25	Análisis de Vulnerabilidades Centralizado	La solución antivirus deberá realizar tareas de análisis automático de vulnerabilidades para detectar vulnerabilidades sin parchar en el sistema operativo Windows y de aplicaciones de terceros. Las funciones de búsqueda de vulnerabilidades y administración de parches de deben automatizar el proceso de mitigar las vulnerabilidades de software. Las vulnerabilidades detectadas pueden priorizarse automáticamente y las actualizaciones y los parches pueden

		distribuirse de manera automática
26	Administración de activos hardware y software centralizado	La solución debe permitir la administración de los activos de hardware y software. Todos los dispositivos de la red deben detectarse y registrarse automáticamente en inventarios de hardware y software. El inventario de hardware deberá contener información detallada sobre cada dispositivo, mientras que el inventario de software ayudará a controlar el uso de aplicaciones y a bloquear las que no están autorizadas.
27	Instalación de Software de Terceros de forma centralizada	La solución debe permitir la distribución de aplicaciones, mediante la implementación centralizada (instalación) de software que no sean de la solución (software de terceros).
28	Implementación de Sistemas Operativos	La solución debe permitir la automatización y optimización de la implementación de sistemas operativos, por tal debe automatizar y centralizar la creación, el almacenamiento y la clonación y distribución de imágenes de sistema operativo. La solución debe de ofrecer funciones automáticas para crear y clonar imágenes de equipo, debe ayudar en optimizar la implementación de sistemas operativos.
ATRIBUTOS EXTERNOS		
29	Distribución descentralizada para oficinas remotas	La solución debe apoyar en la reducción del tráfico en tareas de distribución remota; mediante estaciones de trabajo asignadas como agentes de actualización para oficinas remotas.
30	Integración con SIEM	La solución deberá Integrarse con sistemas SIEM, por tal deberá ser capaz de integrarse a los principales sistemas SIEM.

31	Actualizaciones de Windows	La solución antivirus debe sincronizar con regularidad los datos de las actualizaciones y revisiones de Microsoft para distribuirlas a sus sistemas de forma automática. Para muchas aplicaciones que no son de Microsoft, la solución antivirus deberá proporcionar otras formas de sincronización de para parchar vulnerabilidades.
32	Herramientas de soporte remoto	La solución debe ofrecer herramientas de acceso remoto que apoye a la rápida resolución de problemas en cualquier equipo de la red corporativa mediante el protocolo RDP
33	Descubrimiento de dispositivos en la red	La solución deberá tener la capacidad de descubrir dispositivos de forma automática, que permita controlar quienes pueden acceder a la red corporativa y quiénes no. Además, de comprobar fácilmente si el dispositivo de cada usuario cumple o no con sus políticas de seguridad corporativas y bloquear el acceso a la red a todo dispositivo que no lo haga. Posibilidad de crear un portal cautivo para acceso a internet de los dispositivos visitantes.
34	Plataformas soportadas por el software de gestión	El software de gestión debe soportar Windows Server 2012 R2 o 2016.
35	Creación de Grupos administrativos	El producto debe ser capaz crear grupos administrativos y agregar a ellos automáticamente una PC nueva que ingresa a la red.
36	Instalación automática del software antivirus	El producto debe ser capaz de automáticamente instalar el antivirus en aquellas PC's nuevas que ingresen a la red.
40	Monitoreo Centralizado	La solución antivirus debe de proporcionar una visibilidad detallada de todos activos de TI: Monitorear el estado de seguridad de los sistemas, aplicar ajustes de seguridad necesarios, centralizar aprovisionamiento de licencias de software y detectar infracciones a las condiciones de licencia
41	Despliegue centralizado de actualizaciones de la solución	Actualizaciones descargadas centralizadamente, para que clientes actualicen desde un servidor de administración sus definiciones de virus, phishing, spam, actualización de parches del producto entre otras.

42	Gestión de vulnerabilidades y parches de software de terceros	La solución debe permitir realizar análisis exhaustivos avanzados de vulnerabilidades combinado con distribución automatizada de parches de software de terceros
43	Despliegue de software de terceros en remoto	Instalación y remoción de software de la solución de software de terceros de forma centralizada en los equipos cliente, incluso en sucursales
44	Network Admission Control (NAC)	La solución deberá soportar el control de admisión a la red (NAC), permitiendo crear una política de red de invitados
45	Despliegue de imágenes de sistemas operativos y aplicaciones	La solución de gestión deberá permitir la creación, almacenamiento y despliegue de imágenes de sistema desde una ubicación centralizada
46	Gestión de hardware, software y licencias	La solución de gestión deberá proporcionar informes de inventario de hardware y software; contribuyendo a mantener el control de las obligaciones de licencia de software
37	Soporte Wake on LAN	Soporte para Wake on LAN y Apagado de la PC, permitiendo a las maquinas prenderse /apagarse ante un escaneo programado.
38	Generación de Backups	La consola debe ser capaz de permitir realizar un backup de las configuraciones realizadas en el sistema
39	Soporte SNMP	El producto debe de poder enviar notificaciones vía SNMP
47	Generación de Alertas	El producto debe ser capaz de generación de alertas ante un evento específico mediante el envío de un correo, el envío de mensajes de red o la ejecución de un archivo. Generar eventos de infecciones y ser notificados por medios como alertas de registro y correo electrónico.
48	Reportes	Los reportes deberán ser gráficos para la toma de decisiones y deberán ser mostrados en formatos XML, PDF o HTML, los cuales pueden ser programados para envío por correo
49	Facilidad de Uso y Capacitación	El software debe ser de fácil uso, y de sebe considerar una capacitación para realizar una administración eficiente y segura de la solución antivirus

50	Soporte	El software debe contar con un soporte por el período de vigencia de la licencia, dicho soporte deberá ser responsabilidad el proveedor y del fabricante

Tabla 01: Atributos a considerar para el Análisis Técnico

Luego definimos los puntajes válidos de cada atributo (de acuerdo a los criterios de especificaciones y cumplimiento de cada uno) definido en la tabla 01:

ITEM	PUNTAJE	DESCRIPCIÓN
1	0	No cumple
2	1	Cumplimiento medio
3	2	Cumplimiento Total

Tabla 02: Valores válidos para los atributos

Luego realizamos el análisis técnico comparativo de las soluciones consideras en el presente documento:

NRO	ATRIBUTO	KASPERSKY	SYMANTEC	ESET
ATRIBUTOS INTERNOS				
1	Modalidad de actualizaciones	2	2	2
2	Protección en tiempo real	2	2	2
3	Soporte a sistemas operativos cliente	2	2	2
4	Soporte a sistemas operativos servidor	2	2	2
5	Soporte a dispositivos móviles	2	2	2
6	Protección contra amenazas de día cero	2	2	2
7	Protección Proactiva en el host	2	2	2
8	Protección Proactiva en la red	2	2	2
9	Sistema de Prevención de Intrusos	2	2	2

10	Escaneos Personalizados	2	2	2
11	Protección por contraseña	2	2	2
12	Componentes de la Solución	2	2	2
13	Antispam a nivel de cliente	2	2	2
14	Control Web	2	2	2
15	Control de Dispositivos	2	2	2
16	Motor Heurístico	2	2	2
17	Cifrado	2	0	0
18	Cifrado - Compatibilidad con dispositivos extraíbles	2	0	0
19	Cifrado - Uso compartido de datos seguros	2	0	0
20	Cifrado - Transparencia para usuarios finales	2	0	0
21	Protección de Correo Corporativo Múltiples plataformas	2	2	2
22	Protección de Correo Corporativo - Filtrado	2	2	2
23	Protección de Correo Corporativo - Protocolos	2	2	2
24	Consola de Administración	2	2	2
25	Análisis de Vulnerabilidades Centralizado	2	2	2
26	Administración de activos hardware y software centralizado	2	2	2
27	Instalación de Software de Terceros de forma centralizada	2	2	2

28	Implementación de Sistemas Operativos	2	0	0
ATRIBUTOS EXTERNOS				
29	Distribución descentralizada para oficinas remotas	2	2	2
30	Integración con SIEM	2	2	2
31	Actualizaciones de Windows	2	2	2
32	Herramientas de soporte remoto	2	0	0
33	Descubrimiento de dispositivos en la red	2	2	2
34	Plataformas soportadas por el software de gestión	2	2	2
35	Creación de Grupos administrativos	2	2	2
36	Instalación automática del software antivirus	2	2	2
40	Monitoreo Centralizado	2	2	2
41	Despliegue centralizado de actualizaciones de la solución	2	2	2
42	Gestión de vulnerabilidades y parches de software de terceros	2	2	2
43	Despliegue de software de terceros en remoto	2	2	2
44	Network Admission Control (NAC)	2	2	2
45	Despliegue de imágenes de sistemas operativos y aplicaciones	2	0	0
46	Gestión de hardware, software y licencias	2	1	1

37	Soporte Wake on LAN	2		2
38	Generación de Backups	2	2	2
39	Soporte SNMP	2	2	2
47	Generación de Alertas	2	2	2
48	Reportes	2	2	2
49	Facilidad de Uso y Capacitación	2	2	2
50	Soporte	2	2	2
	TOTAL	**100**	**83**	**85**

Tabla 03: Comparativa Análisis Técnico

Los productos que pasan los 80 puntos en el análisis técnico, serán considerados para la evaluación costo beneficio, ya que cumplen con los atributos o especificaciones mínimas.

8. Análisis de costo beneficio

Los precios detallados en el siguiente cuadro son referenciales, y no son determinantes para la convocatoria del proceso de selección, ya que la Dirección de Abastecimiento es la responsable de realizar el estudio de mercado correspondiente.

N°	CRITERIOS	KASPERSKY	SYMANTEC	ESET
1	Requiere Licenciamiento	**SI**	**SI**	**SI**
2	Precio de 650 Licencias por tres (03) años	**S/.92,625.00**	**S/.188,500.00**	**S/ 120,347.50**
3	Capacitación en el uso del software	**SI**	**SI**	**SI**
4	Gestión Centralizada	**SI**	**SI**	**SI**

Tabla 03: Costo Beneficio

Fórmula de Cálculo

Puntaje Menor Costo (mc) = 100 Ptos.

*Puntaje Mayor Costo (MC) = (mc/MC)*100*

Evaluación Global

Para realizar el análisis global se ha creído por conveniente asignar un peso de 70% al análisis técnico y un 30% al análisis costo beneficio.

N°	SOLUCIÓN	PUNTAJE ANÁLISIS TÉCNICO	PUNTAJE ANÁLISIS COSTO BENEFICIO	PUNTAJE GLOBAL
1	Kaspersky	100	100	**100**
2	Symantec	83	49.14	**59.30**
3	ESET	85	76.96	**79.38**

Tabla 04: Evaluación Final

9. Conclusiones

- El Centro de Información y Sistemas, tiene la necesidad de adquirir licencias de software antivirus, ante la inminente caducidad de la actual solución de software antivirus que usamos.
- La presente evaluación técnica – costo beneficio se realizó en base a tres soluciones de antivirus los cuales son: Kaspersky Total Security For Business, Symantec Endpoint Protection, y ESET Endpoint Security.
- Las soluciones que han superado los ochenta (80) puntos (puntaje global) de la evaluación técnica – costo beneficio es **Kaspersky Total Security for Business**, la cual se sugiere considerar para el proceso de compra.

10. Firmas

Reinaldo Javier Aliaga Infante
Área de Redes y Servidores