Evaluación para Estandarización de Productos de Software del Archivo General de la Nación

INFORME TÉCNICO N° 001-2016-AGN/AI

1. **NOMBRE DE ÁREA:**
   - Área de Informática.

2. **RESPONSABLES DE LA EVALUACIÓN**
   - Avila Goicochea, Vanessa
   - Esquivel Torres, Luis Joseph

3. **CARGO**:
   - Administrador y Soporte de Hardware, Software y Redes

4. **FECHA**:
   - 28 de Noviembre del 2016

5. **OBJETIVO**

   La presente propuesta de estandarización de Software tiene por objetivo establecer un marco de uso obligatorio en el Archivo General de la Nación (AGN) de modo que se adquieran licencias de software compatibles con los productos actualmente en uso. La presente propuesta de estandarización debe ser aplicable a todas las unidades orgánicas del AGN.

6. **ANTECEDENTES:**

   Desde los primeros equipos adquiridos, a la actualidad, el Archivo General de la Nación ha contado siempre con software propietario, ya sea Microsoft Windows como sistema operativo para servidores y usuarios finales y Microsoft Office como software de ofimática, convirtiéndose por ello un software estándar de hecho. Estos programas de software específicos forman parte de nuestra plataforma tecnológica y son usados como herramientas informáticas para el desarrollo de las actividades administrativas y operativas tales como la gestión de servidores, desarrollo y operación de aplicativos internos y módulos de servicios con otras instituciones, sistema de correo electrónico institucional, gestión y administración de la base de datos, así como software para la gestión administrativa entre otros.

   Por medio de Resolución Jefatural N° 238-2012-AGN/J del 15 de agosto del 2012 se aprueba la estandarización del uso del software Windows Server, Microsoft Windows, Microsoft Office y ESET SMART SECURITY, el cual tiene una vigencia de 5 años para el caso de los tres primeros y de dos para el último.

   Por medio de Resolución Jefatural N° 286-2014-AGN/J del 25 de agosto del 2014 se aprueba la estandarización del uso del software Microsoft Exchange, el cual tiene una vigencia de 3 años.

   Por medio de Resolución Jefatural N° 287-2014-AGN/J del 25 de agosto del 2014 se aprueba la estandarización del uso del software Microsoft Project, Microsoft Visio, Adobe Photoshop, Adobe Ilustrator, Adobe InDesign y Adobe Acrobat Professional, los cuales tienen una vigencia de 5 años.

   Por medio de Resolución Jefatural N° 373-2014-AGN/J del 23 de Octubre del 2014 se aprueba la estandarización del uso del software ESET ENDPOINT PROTECTION ADVANCED, el cual tiene una vigencia de 2 años.

7. **JUSTIFICACIÓN:**

El Archivo General de la Nación es la entidad quien tiene la responsabilidad de conducir el desarrollo del Sistema Nacional de Archivos, orientado a la conservación, incremento, protección y servicio del Patrimonio Documental de la Nación a través de la técnica archivística, modernización de los archivos y capacitación especializada a fin de optimizar los servicios archivísticos y servir como fuente de información e investigación en apoyo a la educación, cultura y gestión pública y privada.

El Archivo General de la Nación, cuenta con una solución antivirus conformada por 350 licencias del producto ESET ENDPOINT PROTECTION ADVANCED que viene funcionando desde el año 2014, la cual cuenta con una consola de administración centralizada que cubren las computadoras de usuarios, portátiles y los servidores Windows. La adquisición de dichas licencias se realizó por medio de un proceso de estandarización la cual se oficializa mediante Resolución Jefatural N° 373-2014-AGN/J, otorgando al producto ESET ENDPOINT PROTECTION ADVANCED el uso oficial en las equipos de cómputo del AGN por un periodo de 2 años. Al cumplirse el periodo establecido para dicha estandarización, se hace necesario realizar una nueva evaluación para la adquisición del software antivirus.

Es importante contar con esta herramienta tecnológica por la seguridad al interior de la red de cómputo del Archivo General de la Nación, ya que permite mitigar los efectos producidos por virus informático y sus variantes. Por esta razón es de vital importancia renovar las licencias antivirus.

Entre los principales motivos para la presente justificación de estandarización de software se encuentran:

- Asegurar compatibilidad en el flujo de información y comunicaciones entre usuarios.
- Garantizar y mantener la funcionalidad y operatividad de nuestra infraestructura de software pre-existente.
- Costos en los que incurría el AGN en el proceso de implementación nuevas soluciones tecnológicas.

8. **ALTERNATIVAS (Anexo 1).**

En base a las investigaciones realizadas a través de Internet (Pag. Web Oficiales) y de la información proporcionada por los fabricantes de soluciones de antivirus se ha considerado a las siguientes soluciones como las mejores alternativas para su implementación en Archivo General de la Nación.

ARCHIVO GENERAL DE LA NACIÓN Área de Informática

- Eset Endpoint Antivirus
- Kaspersky endpoint Security Business Select.
- Mcafee Endpoint Protection Suite

9. **ANÁLISIS COMPARATIVO (Anexo 2).**

El análisis comparativo técnico se hizo sobre software comercial con instalador descargable de internet en calidad de prueba, y teniendo en consideración la experiencia en el uso de cada herramienta por parte del personal del Área de Informática de la entidad

a. **Propósito de evaluación**
   Validar que la herramienta seleccionada sea la más conveniente para el uso en el Archivo General de la Nación.
b. **Identificar el tipo de producto**
   Los software detallados en el punto N° 8 del presente informe, cumplen con la necesidad de los profesionales del Archivo General de la Nación.
c. **Modelo de calidad**
   Se aplicó para este fin el Modelo de calidad de software, metodología establecida en la Guía de evaluación de software para la administración pública", aprobada por Resolución Ministerial 139-2004-PCM.

Se precisa que para las evaluaciones se ha establecido un puntaje técnico mínimo que debe alcanzar cada producto evaluado (70 puntos) para poder ser considerado como apto para su implementación, si el producto no supera dicho puntaje técnico no será aceptado por no contar con la funcionalidad básica requerida.

9.1 Características técnicas mínimas y escalas para las métricas

Tipo de Calidad	Características	Métricas	PUNTAJE MÍNIMO (60 puntos)	PUNTAJE MÁXIMO (100 puntos)
CALIDAD INTERNA Y EXTERNA	FUNCIONABILIDAD	Solución Antivirus Multiplataforma para Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10 y Windows Server 2003/2008/2012. Deberá Soportar las versiones de 32 y 64 bits.	3	4
		Bloqueo y Eliminación de Malware como virus, spyware, adware, rootkits, bots, etc.	3	4
		El antivirus deberá incluir una protección antivirus a nivel HTTP que incluya adicionalmente un filtro de páginas web (Listas negras y blancas) para el bloqueo de URL's no permitidos, la misma que podrá ser editada por los usuarios y/o administrador de la red.	3	4
		Deberá de tener un componente que busque virus en el protocolo POP3 (descarga de e-mails), SMTP (envío de correos), IMAP (descarga y envío de correos) y Protocolo HTTP (navegación en Internet).	3	4
		Deberá permitir la protección y bloqueo de medios extraíbles tales como dispositivos de almacenamiento USB, CD's, disquetes, etc.	3	4
		El antivirus ofertado deberá contar con alguna tecnología que evite que los códigos maliciosos desactiven los componentes del antivirus.	3	4
		El antivirus ofertado deberá permitir bloquear ciertas secciones críticas del Registro de Windows, esto con la finalidad de evitar que los códigos maliciosos desactiven o vulneren la funcionalidad del antivirus.	3	4
		El antivirus deberá incluir una protección antivirus a nivel HTTP que incluya adicionalmente una Gestión de direcciones HTTP, donde se podrá definir listas de direcciones que se bloquearán, permitirán o excluirán del análisis.	2	4
		El antivirus deberá tener un sistema de verificación de parches y/o actualizaciones críticas de Windows, emitiendo alertas cuando estas estén disponibles para su descarga.	2	3
		Notificar los eventos de virus por diferentes medios (email, etc.).	2	3
		Debe incluir actualizaciones y/o parches los cuales se deberán descargar de internet sin costo alguno.	2	4
		Deberá contar con un cliente configurable para estaciones de trabajo de tecnologías antiguas como: Core 2 Duo con capacidad de memoria de al menos 64 MB.	2	3

	USABILIDAD	El antivirus ofertado deberá de soportar actualizaciones automáticas de una versión anterior de software. Es decir, para actualizar a una nueva versión no es necesario desinstalar la versión existente.	2	4
		Deberá de admitir múltiples configuraciones para permitir la distribución de carga incrementando la escalabilidad del sistema.	2	4
		El personal tiene capacitaciones y cuenta con experiencia en el uso del producto del software	2	4
		La consola del antivirus ofertado deberá de instalarse sobre el sistema operativo Microsoft Windows, sea esta una estación de trabajo o un servidor.	2	4
		Deberá de admitir métodos de instalación remota – los administradores podrán instalar a los equipos en línea.	3	4
		Los administradores de la consola tendrán la capacidad de cambiar la configuración de múltiples clientes a la vez, ejecutar silenciosas revisiones por demanda a clientes específicos sin la intervención o conocimiento del usuario final, forzar a los clientes a actualizarse en tiempo real y crear grupos de clientes para facilitar la ejecución de tareas de actualización.	2	4
		Los administradores de la consola podrán generar una amplia variedad de reportes predefinidos o personalizados. Los reportes podrán ser obtenidos de forma automática o repetitivamente a intervalos de tiempo predefinidos. Podrán ser filtrados por clientes específicos y/o virus. Todos los reportes deberán de estar en formato HTML para su fácil publicación en la Intranet corporativa y la presentación de informes mensuales.	2	4
		Los administradores de la consola del antivirus ofertado podrán configurar remotamente clientes del antivirus ofertado.	2	4
	EFICIENCIA	Bajos requerimientos de recursos (Procesamiento, memoria y disco duro).	2	4
CALIDAD EN USO	PRODUCTIVIDAD	No deberá consumir muchos recursos de memoria y procesador en los equipos de los usuarios.	2	4
		El producto de software permite a los usuarios lograr las metas especificadas con exactitud e integridad, en el contexto requerido.	2	4
	SEGURIDAD	El usuario no debe poder realizar una configuración particular del antivirus a menos que el administrador le otorgue privilegios.	2	3
	PORTABILIDAD	Facilidad de instalación	2	4
		El producto de software deberá coexistir con otros productos de software independientes dentro de un mismo entorno, compartiendo recursos comunes.	2	4

9.2 Análisis Comparativo productos de software Antivirus

Valorización de cada una de las alternativas, según los atributos establecidos en el punto 9.1

Tipo de Calidad	Características	Métricas	Eset Endpoint Antivirus	Mcafee Endpoint Protection Suite	Kaspersky endpoint Security Business
CALIDAD INTERNA Y EXTERNA	FUNCIONABILIDAD	Solución Antivirus Multiplataforma para Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10 y Windows Server 2003/2008/2012. Deberá Soportar las versiones de 32 y 64 bits.	4	4	4
		Bloqueo y Eliminación de Malware como virus, spyware, adware, rootkits, bots, etc.	4	4	4
		El antivirus deberá incluir una protección antivirus a nivel HTTP que incluya adicionalmente un filtro de páginas web (Listas negras y blancas) para el bloqueo de URL's no permitidos, la misma que podrá ser editada por los usuarios y/o administrador de la red.	4	4	4
		Deberá de tener un componente que busque virus en el protocolo POP3 (descarga de e-mails), SMTP (envío de correos), IMAP (descarga y envío de correos) y Protocolo HTTP (navegación en Internet).	4	4	4
		Deberá permitir la protección y bloqueo de medios extraíbles tales como dispositivos de almacenamiento USB, CD's, disquetes, etc.	4	4	4
		El antivirus ofertado deberá contar con alguna tecnología que evite que los códigos maliciosos desactiven los componentes del antivirus.	4	4	4
		El antivirus ofertado deberá permitir bloquear ciertas secciones críticas del Registro de Windows, esto con la finalidad de evitar que los códigos maliciosos desactiven o vulneren la funcionalidad del antivirus.	3	3	3
		El antivirus deberá incluir una protección antivirus a nivel HTTP que incluya adicionalmente una Gestión de direcciones HTTP, donde se podrá definir listas de direcciones que se bloquearán, permitirán o excluirán del análisis.	4	3	4
		El antivirus deberá tener un sistema de verificación de parches y/o actualizaciones críticas de Windows, emitiendo alertas cuando estas estén disponibles para su descarga.	3	3	3

		Notificar los eventos de virus por diferentes medios (email, etc.).	3	3	3
		Debe incluir actualizaciones y/o parches los cuales se deberán descargar de internet sin costo alguno.	4	4	4
		Deberá contar con un cliente configurable para estaciones de trabajo de tecnologías antiguas como: Core 2 Duo con capacidad de memoria de al menos 64 MB.	3	2	3
	USABILIDAD	El antivirus ofertado deberá de soportar actualizaciones automáticas de una versión anterior de software. Es decir, para actualizar a una nueva versión no es necesario desinstalar la versión existente.	3	2	3
		Deberá de admitir múltiples configuraciones para permitir la distribución de carga incrementando la escalabilidad del sistema.	4	3	3
		El personal tiene capacitaciones y cuenta con experiencia en el uso del producto del software	4	3	4
		La consola del antivirus ofertado deberá de instalarse sobre el sistema operativo Microsoft Windows, sea esta una estación de trabajo o un servidor.	4	3	4
		Deberá de admitir métodos de instalación remota – los administradores podrán instalar a los equipos en línea.	3	3	3
		Los administradores de la consola tendrán la capacidad de cambiar la configuración de múltiples clientes a la vez, ejecutar silenciosas revisiones por demanda a clientes específicos sin la intervención o conocimiento del usuario final, forzar a los clientes a actualizarse en tiempo real y crear grupos de clientes para facilitar la ejecución de tareas de actualización.	4	3	3
		Los administradores de la consola podrán generar una amplia variedad de reportes predefinidos o personalizados. Los reportes podrán ser obtenidos de forma automática o repetitivamente a intervalos de tiempo predefinidos. Podrán ser filtrados por clientes específicos y/o virus. Todos los reportes deberán de estar en formato HTML para su fácil publicación en la Intranet corporativa y la presentación de informes mensuales.	4	4	4
		Los administradores de la consola del antivirus ofertado podrán configurar	3	3	3

		remotamente clientes del antivirus ofertado.			
	EFICIENCIA	Bajos requerimientos de recursos (Procesamiento, memoria y disco duro).	3	2	2
CALIDAD EN USO	PRODUCTIVIDAD	No deberá consumir muchos recursos de memoria y procesador en los equipos de los usuarios.	3	2	2
		El producto de software permite a los usuarios lograr las metas especificadas con exactitud e integridad, en el contexto requerido.	3	3	3
	SEGURIDAD	El usuario no debe poder realizar una configuración particular del antivirus a menos que el administrador le otorgue privilegios.	3	3	3
	PORTABILIDAD	Facilidad de instalación	2	3	2
		El producto de software deberá coexistir con otros productos de software independientes dentro de un mismo entorno, compartiendo recursos comunes.	3	4	3
TOTAL			90	83	86

9.3 ANALISIS COMPARATIVO COSTO BENEFICIO (Anexo 3).

Se ha realizado las consultas con diversas empresas, los costos mayores o menores en que se incurran para remplazar el software en uso, no son mesurables respecto del riesgo existente por la sustitución del software actual en uso, el que impactaría en los procesos productivos y administrativos que utilizan estas herramientas como insumo principal.

N°	Descripción	Licencia	Costo S/.
1	Eset Endpoint Antivirus	350	9582
2	Kaspersky endpoint Security Business Select	350	21000
3	Mcafee Endpoint Protection Suite	350	12310

Los precios del software detallados son referenciales, a fin de poder determinar el costo beneficio de los mismos. Se recomienda que la Unidad de Abastecimiento realice un estudio de mercado.

10. CONCLUSIONES

Por lo expuesto, el software Antivirus en mención cumple con todos los requisitos mínimos especificados y además por ser la mejor opción para satisfacer la necesidad de Seguridad del Archivo General de la Nación, se concluye y recomienda adquirir el siguiente producto de software Antivirus en su última versión:

Ítem	Software Antivirus
Software Antivirus	ESET ENDPOINT ANTIVIRUS

La vigencia de la presente estandarización será evaluada en un lapso de 1 año.

ANEXO 1

ALTERNATIVAS

ENDPOINT ANTIVIRUS

ESET Endpoint Antivirus, basado en la multipremiada tecnología de ESET NOD32®, proporciona una potencia de detección superior para su empresa.

Su baja demanda de recursos del sistema y su capacidad de virtualización mantienen el sistema en su máximo rendimiento.

Mantenga la seguridad de sus dispositivos offline bajo control y personalice las opciones de exploración y de actualización como lo crea necesario. Controle todo sin esfuerzo con nuestra herramienta de administración remota, totalmente nueva y fácil de usar.

Protección de endpoints

Antivirus y antispyware	Elimina todos los tipos de amenazas, incluyendo virus, rootkits, gusanos y spyware. **Exploración opcional basada en la nube:** Creación de listas blancas de archivos seguros según la base de datos de reputación de archivos en la nube, para lograr una mejor detección y una exploración más rápida. Solo se envía a la nube la información de archivos ejecutables y de archivos comprimidos; el envío se realiza en forma anónima.
Soporte para la virtualización	La Caché local compartida de ESET almacena metadatos sobre los archivos ya explorados dentro de cada entorno virtual con la finalidad de no volver a explorar los mismos archivos nuevamente y, de esa forma, acelerar la velocidad de exploración. Las actualizaciones de los módulos y de la base de datos de firmas de virus de ESET se almacenan fuera de la ubicación predeterminada, por lo tanto no se deben descargar cada vez que el estado de la máquina virtual se revierte a la instantánea predeterminada.
Sistema de prevención de intrusiones basado en el host (HIPS)	Permite definir reglas para el registro del sistema, los procesos, las aplicaciones y los archivos. Suministra protección ante la manipulación indebida y detecta amenazas basándose en la conducta del sistema.
Bloqueo de exploits	Refuerza la seguridad de las aplicaciones en los sistemas de los usuarios, por ej., navegadores Web, lectores de PDF, clientes de correo electrónico o componentes de MS Office, que suelen ser los objetivos de ataque más comunes. Monitorea la conducta de los procesos en busca de actividades sospechosas típicas de los exploits. Refuerza la protección ante ataques dirigidos y exploits desconocidos hasta el momento, es decir, ataques zero-day.
Exploración avanzada de memoria	Monitorea la conducta de los procesos maliciosos y los explora cuando se muestran en memoria. Así se logra una prevención efectiva contra las infecciones, incluso ante los tipos más furtivos de malware.
Protección para plataformas múltiples	Las soluciones de seguridad de ESET para Windows son capaces de detectar amenazas para Mac OS y viceversa, de modo que suministran una mejor protección en entornos de plataformas múltiples.

Protección del acceso a los datos

Anti-Phishing	Protege a los usuarios finales de los sitios Web falsos que se hacen pasar por sitios confiables para obtener información confidencial, como nombres de usuario, contraseñas o detalles bancarios y de tarjetas de crédito.
Control de dispositivos	Bloquea el acceso al sistema para los dispositivos no autorizados (unidades de CD, DVD y USB). Permite crear reglas para grupos de usuarios con el objetivo de cumplir con las normativas y políticas corporativas. La regla de bloqueo de advertencia le notifica al usuario final que se bloqueó su dispositivo y le da la opción de acceder a él pero registrando la actividad.

Opciones de exploración y actualización

Exploración en estado inactivo	Realiza las exploraciones completas en forma proactiva mientras el equipo no está en uso, contribuyendo a un mejor rendimiento del sistema. Llena la caché local y ayuda a acelerar las exploraciones futuras.
Primera exploración tras la instalación	Suministra la opción de ejecutar una exploración bajo demanda de baja prioridad 20 minutos después de la instalación del programa, lo que asegura que el sistema esté protegido desde el comienzo.
Reversión de la actualización	Permite revertir el sistema a una versión anterior de los módulos de protección y de la base de datos de firmas de virus. Le brinda la posibilidad de congelar las actualizaciones como lo desee: elija hacer una reversión temporal o demorar las actualizaciones hasta su modificación manual.
Actualizaciones postergadas	Ofrece la opción de realizar las descargas desde 3 servidores de actualización especializados: actualizaciones previas a su lanzamiento (usuarios de versiones beta), lanzamientos regulares (recomendados para sistemas no críticos) y lanzamientos postergados (recomendados para los sistemas críticos de las empresas; aproximadamente 12 horas después del lanzamiento regular).
Servidor de actualización local	Ahorra el ancho de banda de la empresa, ya que descarga las actualizaciones una sola vez, a un servidor mirror local. Los trabajadores móviles actualizan sus dispositivos directamente desde el servidor de actualización de ESET cuando el mirror local no está disponible. Cuenta con soporte para canales de comunicación seguros (HTTPS).

SOPORTE TÉCNICO GRATUITO LOCAL.

Haga más con la ayuda de nuestros especialistas.

Soporte técnico disponible cuando lo necesita, en su idioma.

Usabilidad

RIP & Replace	Durante la instalación de ESET Endpoint Solutions, la solución detecta si hay otros programas de seguridad y los desinstala. Es compatible con sistemas de 32 y de 64 bits.
Visibilidad personalizable de la interfaz gráfica del usuario	La visibilidad de la interfaz gráfica del usuario (GUI) en los equipos de los usuarios finales puede configurarse en: Completa, Mínima, Manual o Silenciosa. Es posible hacer que la solución de ESET sea totalmente invisible para el usuario final, incluyendo la eliminación del icono en la bandeja y de las ventanas de notificaciones. Al ocultar la GUI por completo, el proceso "egui.exe" directamente no se ejecuta; esto genera que la solución de ESET consuma aún menos recursos del sistema.
ESET License Administrator	Permite el manejo de todas las licencias en forma transparente, desde un mismo lugar, a través de un navegador Web. Podrá combinar, delegar y administrar todas las licencias de manera centralizada en tiempo real, incluso aunque no esté usando ESET Remote Administrator.
Soporte para pantallas táctiles	Ofrece compatibilidad con pantallas táctiles y permite la visualización en pantallas de alta resolución. Más márgenes y reorganización completa de los elementos de la GUI. Acceso a las acciones básicas utilizadas con mayor frecuencia desde el menú en la bandeja.
Bajo impacto en el sistema	Ofrece protección comprobada a la vez que deja disponibles más recursos del sistema para los programas que los usuarios finales ejecutan con más frecuencia. Puede desplegarse en máquinas más viejas sin necesidad de actualizarlas, por lo que ayuda a extender la vida útil del hardware. El modo de alimentación a batería conserva la vida de la batería en equipos portátiles que se usan fuera de la oficina.
Soporte para idiomas de derecha a izquierda	Soporte nativo para idiomas de derecha a izquierda (por ej., árabe), garantizando la utilidad óptima para el usuario final.
Administración remota	Las soluciones ESET Endpoint Solutions pueden administrarse en su totalidad desde ESET Remote Administrator. Haga el despliegue, ejecute tareas, determine políticas, recopile registros y obtenga notificaciones e información general de la seguridad de la red: todo a través de una única consola de administración basada en la Web.

McAfee Endpoint Protection Suite

Proteja los sistemas Microsoft Windows, Mac y Linux con la seguridad esencial de endpoints y datos.

Puntos clave

- Protección fundamental con seguridad consolidada de endpoints y datos
- Reducción del tiempo y el esfuerzo invertidos en desplegar y administrar la seguridad
- Protección de los endpoints con defensas inteligentes que luchan contra todas las amenazas avanzadas en tiempo real

Proteger los datos significa mantener varias capas de defensa que garanticen siempre su seguridad cuando se desplacen por su entorno. Pero no solo debe proteger sus endpoints frente a amenazas avanzadas, también debe evitar la pérdida de datos y garantizar el cumplimiento de las normativas. McAfee® Endpoint Protection Suite — parte de la oferta de productos de Intel® Security — integra estas funciones imprescindibles en un único entorno de fácil manejo, ideal para proteger los sistemas y los datos, y al mismo tiempo facilitar el despliegue, la supervisión y los cambios a los administradores.

Las aplicaciones basadas en la Web y el correo electrónico son esenciales para casi cualquier empresa en la actualidad, y los ciberdelincuentes lo saben. La protección en todo el ciclo de vida de defensa frente a amenazas requiere una seguridad que cubra varios sistemas, dispositivos y sistemas operativos.

El caso de la protección de los datos es similar, sin embargo, hay además riesgos físicos y provocados por el usuario que pueden derivarse del uso de soportes extraíbles, errores del personal interno o incluso por un empleado insatisfecho que copia propiedad intelectual o datos de clientes con fines malintencionados.

McAfee Endpoint Protection Suite integra perfectamente varias soluciones de seguridad, de eficacia probada, para gestionar todos estos riesgos, mejorando la eficiencia operativa y el ahorro de costes cómodamente con una sola solución.

Defensas inteligentes y colaborativas

Las empresas requieren una estrategia para la protección, la detección de las amenazas y la corrección de sus efectos, así como un marco de seguridad que facilite la colaboración de los componentes de seguridad frente a los ataques selectivos con el fin de garantizar una rápida detección y solución.

McAfee Endpoint Security se comunica con varias tecnologías de defensa de endpoints en tiempo real para analizar y colaborar frente a las amenazas nuevas y avanzadas, bloqueándolas y deteniéndolas rápidamente antes de que afecten a sus sistemas o usuarios. Su plataforma ayuda a eliminar las tecnologías duplicadas y a conectar las demás soluciones de Intel Security para facilitar la administración y reforzar las defensas. Además, McAfee Global Threat Intelligence proporciona información procedente de la mayor base de datos de observaciones y análisis del mercado.

intel Security

Por qué Intel Security

- Ofrecemos a los administradores una experiencia verdaderamente centralizada.
- Nuestras plataformas de seguridad y de endpoints integradas permiten eliminar las redundancias, conectar con otras soluciones y ofrecer una arquitectura ampliable sobre la que se puede crecer.
- McAfee Global Threat Intelligence ofrece el mayor volumen de información sobre amenazas del mercado. Vemos y protegemos más que nadie.

Protección avanzada del correo electrónico contra virus y spam

Nuestra solución analiza sus mensajes de correo electrónico entrantes y salientes para interceptar spam, contenidos inapropiados y virus. Podemos poner en cuarentena el correo electrónico de carácter sospechoso para evitar que las nuevas amenazas afecten a su red y a sus usuarios. Y la protección antivirus garantiza la seguridad de su servidor de correo electrónico para impedir que el malware llegue a la bandeja de entrada de los usuarios.

Control total de dispositivos

Con nosotros es posible evitar que los datos fundamentales salgan de su empresa a través de soportes extraíbles, como unidades USB, iPods, dispositivos Bluetooth, o CD y DVD grabables. Nuestras herramientas le ayudan a supervisar y controlar las transferencias de datos desde todos los equipos de sobremesa, incluso cuando no están conectados a la red corporativa.

Firewall integrado

Controle las aplicaciones de escritorio que pueden acceder a la red para detener los ataques propagados por esta vía y los consiguientes tiempos de inactividad. Nuestro firewall integrado bloquea el tráfico entrante no solicitado y controla el tráfico saliente, incluso durante el inicio mientras se aplica la directiva de firewall. También se puede desplegar y administrar directivas de firewalls según la ubicación, para garantizar una protección completa y el cumplimiento de las normativas.

Seguridad de la Web proactiva

En Internet, muchas amenazas son invisibles y pasan desapercibidas para los usuarios. Contribuya a garantizar el cumplimiento de las normativas y a reducir los riesgos asociados a la navegación por Internet. Para ello, alerte a los usuarios sobre los sitios web maliciosos antes de que los visiten. También puede autorizar o bloquear el acceso a sitios web por usuario y grupo, y controlar el acceso de los usuarios a sitios confidenciales o inapropiados, como los de juegos y contenido para adultos. Por último, es posible bloquear URL privadas y se admiten las últimas versiones de múltiples navegadores web.

Reducción de costes operativos gracias a una administración centralizada

Todas las funciones de McAfee Endpoint Protection Suite se administran con el software McAfee ePolicy Orchestrator® (McAfee ePO™), una plataforma centralizada que administra la seguridad, implementa la protección y reduce el coste de las operaciones de seguridad. Basada en la Web para facilitar el acceso, ofrece seguridad inteligente para agilizar y optimizar la toma de decisiones y reforzar el control.

El software McAfee ePO puede reducir el coste de la gestión de la seguridad de TI y el cumplimiento de normativas, ya que ofrece una visibilidad más rápida y una administración más sencilla de todos los endpoints de su entorno, así como de otras funciones de protección de Intel Security y más de 130 soluciones de seguridad de terceros.

Este concepto abierto de la infraestructura de administración se basa en un único agente y una sola consola. En comparación con las soluciones individuales de generaciones anteriores, nuestro modelo racionalizado simplifica enormemente la instalación y el mantenimiento de las medidas de defensa, así como de sus reglas y directivas. Además, elimina el impacto que tiene en los sistemas la actuación de varios agentes y los conflictos de decisiones derivados del uso de distintas consolas. Cuando se deben revisar las directivas, las actualizaciones se realizan de manera rápida, precisa y coherente.

Además, puede correlacionar las amenazas, ataques y eventos de la seguridad de endpoints, red y datos, así como las auditorías de cumplimiento de normativas con el fin de mejorar la relevancia y la eficacia de los esfuerzos de protección y los informes de cumplimiento de normativas. Ningún otro proveedor posee una única plataforma de administración integrada que cubra todos estos dominios de seguridad.

Despliegue rápido y sencillo

Mejora la protección sin demora. El instalador EASI pone en funcionamiento esta protección robusta con solo unos cuantos clics.
La integración con el software McAfee ePO permite desplegar y administrar la seguridad con un único entorno.

Migrar es fácil

Los entornos que utilizan versiones actuales del software McAfee ePO, McAfee® VirusScan® Enterprise y McAfee Agent pueden disfrutar de nuestra herramienta de migración automática para migrar sus directivas existentes a McAfee Endpoint Security 10 en cuestión de 20 minutos o menos*.

Más información

Para obtener más información, visite **www.mcafee.com/es/products/endpoint-protection/index.aspx**.

Función	Por qué necesita esta solución
Administración integrada unificada	El software McAfee ePO proporciona visibilidad instantánea de los eventos y del estado de seguridad, y facilita el acceso directo a la administración para controlar de manera centralizada todas sus herramientas de seguridad y de cumplimiento de normativas.
Multiplataforma	Protege la amplia gama de endpoints que necesitan los usuarios avanzados y móviles, incluidos los sistemas Mac, Linux y Microsoft Windows.
Control de dispositivos	Le permite supervisar y restringir los datos que se copian en dispositivos y soportes de almacenamiento extraíbles para impedir que escapen al control de la empresa.
Firewall integrado	Garantiza la prevención de ataques procedentes de la red y la exclusiva autorización del tráfico legítimo.
Antimalware	Bloquea virus, troyanos, gusanos, adware, spyware y otros programas potencialmente no deseados que roban datos confidenciales y sabotean la productividad de los usuarios.
Antispam	Ayuda a eliminar el spam, que puede inducir a usuarios desprevenidos a visitar sitios que distribuyen malware y utilizan técnicas de phishing.
Seguridad de servidores de correo electrónico	Protege el servidor del correo electrónico e intercepta el malware antes de que llegue al buzón de entrada del usuario.
McAfee Web Control con filtrado de URL y búsquedas seguras	Ayuda a garantizar el cumplimiento de las normativas y a reducir los riesgos asociados a la navegación por Internet. Para ello, alerta a los usuarios sobre los sitios web maliciosos antes de que los visiten, dejando que sean los administradores los que decidan autorizar o bloquear el acceso a los sitios web.

intel Security

* El tiempo de migración depende de las directivas existentes y del entorno actual.

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com

420_0816

▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Select

Herramientas para dar soporte a un personal laboral móvil, garantizar el cumplimiento con las políticas de seguridad de TI y bloquear el malware.

El nivel de protección "Select" de Kaspersky incluye implementación y protección para dispositivos móviles mediante Mobile Device Management (MDM) y funciones anti-malware para móviles. Las herramientas de control de terminales (web, dispositivos y aplicaciones) permiten a tu organización aplicar la política de TI, lo que mantiene seguros los elementos esenciales de tu entorno de TI.

Las funciones de protección y gestión que necesitas.

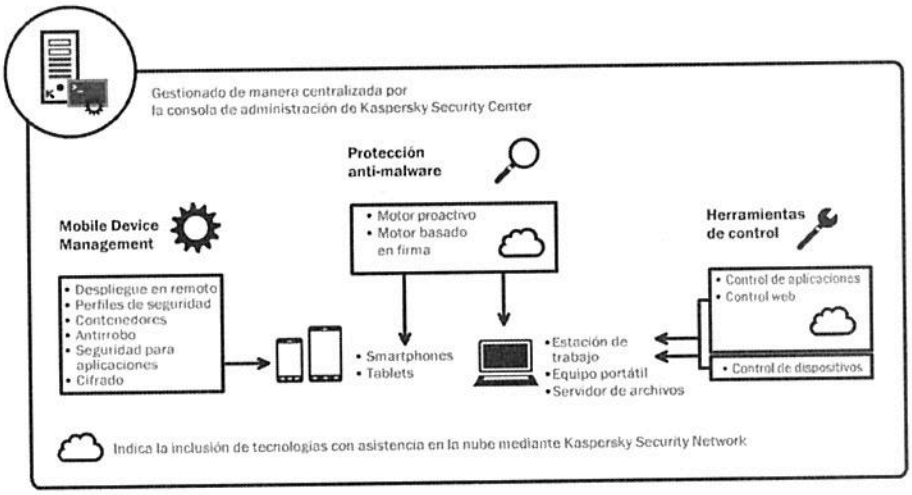
En Kaspersky hemos integrado potentes funciones empresariales en todos los niveles de protección de las soluciones que ofertamos, utilizando siempre una tecnología sencilla e idónea para empresas de cualquier tamaño.

¿Qué nivel de protección es el más adecuado para ti?

- CORE
- **SELECT**
- ADVANCED
- TOTAL

FUNCIONES INCLUIDAS:

- ANTI-MALWARE
- FIREWALL
- PROTECCIÓN CON ASISTENCIA EN LA NUBE MEDIANTE KASPERSKY SECURITY NETWORK
- CONTROL DE APLICACIONES
- MARCADO DE APLICACIONES EN LISTA BLANCA
- CONTROL WEB
- CONTROL DE DISPOSITIVOS
- PROTECCIÓN DE SERVIDORES DE ARCHIVOS
- MOBILE DEVICE MANAGEMENT
- SEGURIDAD PARA TERMINALES MÓVILES



FUNCIONES PRINCIPALES:

POTENTE ANTI-MALWARE PARA TERMINALES
El mejor motor de análisis de Kaspersky funciona en varios niveles del sistema operativo, eliminando el malware de raíz. Kaspersky Security Network (KSN) basado en la nube protege a los usuarios en tiempo real contra nuevas amenazas.

HERRAMIENTAS DE CONTROL FLEXIBLES Y CON GRAN NIVEL DE DETALLE
Una base de datos categorizada basada en la nube que enumera las aplicaciones y las páginas web seguras y no seguras permite al administrador definir y aplicar políticas para aplicaciones y navegación web, mientras que los controles con gran nivel de detalle garantizan que sólo los dispositivos específicos se puedan conectar a los equipos de la red.

EFICAZ IMPLEMENTACIÓN Y SEGURIDAD MÓVIL PARA SMARTPHONES Y TABLETS
La seguridad móvil basada en agentes está disponible para dispositivos móviles Android™, Blackberry®, Symbian y Windows® Mobile. Las políticas y el software para los dispositivos móviles se pueden implementar de forma segura de forma inalámbrica mediante Kaspersky MDM tanto en estos dispositivos como en dispositivos iOS.

ANALIZADOR DE VULNERABILIDADES
Ajustado para indicar vulnerabilidades de hardware y software que podrían suponer una posible exposición a un ataque.

FUNCIONES DE PROTECCIÓN DE TERMINALES:

ACTUALIZACIONES FRECUENTES Y PROTECCIÓN BASADA EN FIRMAS
Método tradicional basado en firmas de eficacia demostrada para detectar amenazas de malware.

ANÁLISIS DE COMPORTAMIENTO DE SUPERVISOR DEL SISTEMA
Ofrece una protección proactiva contra amenazas que aún no se han registrado en las bases de datos de firmas.

PROTECCIÓN CON ASISTENCIA EN LA NUBE
Kaspersky Security Network (KSN) ofrece una respuesta inmediata ante sospechas de amenazas, de forma mucho más rápida que los métodos de protección tradicionales. El tiempo de respuesta de KSN a una amenaza de malware puede ser de tan sólo 0.02 segundos.

SISTEMA DE PREVENCIÓN DE INTRUSIONES BASADO EN HOST (HIPS) CON FIREWALL PERSONAL
Gracias a las reglas predefinidas para cientos de las aplicaciones más comúnmente utilizadas se reduce el tiempo invertido en la configuración del firewall.

CONTROL DE ENDPOINT

CONTROL DE APLICACIONES
Permite a los administradores de TI establecer políticas de autorización, bloqueo o regulación de aplicaciones (o categorías de aplicaciones).

CONTROL WEB
Significa que los controles de navegación basados en terminales hacen un seguimiento del usuario, tanto en la red empresarial como en itinerancia.

CONTROL DE DISPOSITIVOS
Permite a los usuarios establecer, programar y aplicar políticas de datos con controles para dispositivos de almacenamiento extraíbles y otros dispositivos periféricos conectados a un puerto USB o cualquier otro tipo de bus.

LISTAS BLANCAS DINÁMICAS
El envío datos de reputación de archivos en tiempo real de Kaspersky Security Network permite garantizar que las aplicaciones aprobadas estén libres de malware, así como maximizar la productividad de los usuarios.

FUNCIONES DE SEGURIDAD MÓVIL:

INNOVADORAS TECNOLOGÍAS ANTI-MALWARE
La combinación de tecnologías de detección basadas en firma, proactivas y con asistencia en la nube proporciona protección en tiempo real. Mayor seguridad gracias a una navegación segura, a tecnologías antispam y a aplicaciones con tecnología sandbox.

IMPLEMENTACIÓN CON ABASTECIMIENTO INALÁMBRICO
Capacidad para preconfigurar e implementar aplicaciones de forma centralizada mediante el uso de SMS, correo electrónico y ordenadores.

HERRAMIENTAS ANTIRROBO REMOTAS
Las herramientas de vigilancia de SIM, bloqueo remoto, borrado y búsqueda evitan el acceso no autorizado a los datos de la empresa en caso de robo o pérdida de un dispositivo móvil.

CONTROL DE APLICACIONES PARA DISPOSITIVOS MÓVILES
Supervisa las aplicaciones instaladas en un dispositivo móvil, de acuerdo con las políticas de grupo predefinidas. Incluye un grupo de "aplicación obligatoria".

COMPATIBILIDAD CON LOS DISPOSITIVOS PERSONALES DE LOS EMPLEADOS
Los datos y las aplicaciones de la empresa permanecen aislados en contenedores cifrados de apariencia transparente para los usuarios. Estos datos se pueden borrar por separado.

▸LA ÚNICA PLATAFORMA DE SEGURIDAD DEL SECTOR.

Una única consola de gestión
A través de un único "panel de control", el administrador puede ver y gestionar todo el sistema de seguridad: equipos virtuales y dispositivos tanto físicos como móviles.

Una única plataforma de seguridad
Kaspersky Lab ha desarrollado nuestra consola, módulos de seguridad y herramientas de forma interna en lugar de adquirirlos de otras empresas. Eso significa que los programadores que trabajan en el mismo código base han desarrollado tecnologías que interactúan entre sí y funcionan de forma conjunta. Esto se traduce en estabilidad, políticas integradas, generación de informes útiles y herramientas intuitivas.

Un único coste
Todas las herramientas provienen de un único proveedor y se proporcionan mediante una única instalación, para que no tengas que pasar por un nuevo proceso de presupuestación y justificación para alinear tus riesgos de seguridad con tus objetivos empresariales.

NO TODAS LAS FUNCIONES SE ENCUENTRAN DISPONIBLES EN TODAS LAS PLATAFORMAS. Para obtener más información, consulta **www.kaspersky.es**

KESB-S/Versión 0.1/Nov12/Global

KASPERSKY lab

ANEXO 2

ANÁLISIS COMPARATIVO

Security Labs

Lima, 08 de noviembre de 2016

Señores:
ARCHIVO GENERAL DE LA NACIÓN

Atención:
Luis Esquivel

Asunto: Cotización de soluciones de seguridad ESET - **NLEP20161108-42**

ESET, empresa pionera en protección antivirus desde 1987, desarrolla soluciones de seguridad que ayudan a más de 100 millones de usuarios a disfrutar la tecnología de forma segura. Su portafolio de soluciones ofrece a las empresas y consumidores de todo el mundo un equilibrio perfecto entre rendimiento y protección proactiva. La empresa cuenta con una red global de ventas que abarca 180 países y tiene oficinas centrales en Bratislava, Eslovaquia y de Coordinación Global en San Diego, California.

Premios y reconocimientos

Los productos de **ESET** cuentan con una exitosa trayectoria en las pruebas de rendimiento y en las pruebas de detección de **AV-Comparatives**	Gartner reconoce a **ESET** como "**Visionario**" dentro de su famoso Cuadrante Mágico para la protección de endpoints	**ESET** obtuvo la mayor cantidad de premios **VB100** consecutivos por detección de malware entre todos los fabricantes de seguridad para Internet

ARCHIVO GENERAL DE LA NACIÓN Área de Informática

SECURITY LABS, Partner Gold autorizado y certificado de ESET, es una organización especializada en seguridad informática, que ofrece soluciones contra malware. Nuestro equipo técnico/comercial cuenta con más de 15 años de experiencia.

Contamos con personal técnico altamente capacitado y certificado que lo asistirá remotamente, por teléfono y/o de manera presencial en sus oficinas sin ningún costo adicional.

Brindamos entrenamiento técnico al personal de su organización para el correcto uso de las soluciones de ESET, aplicación de buenas prácticas para la gestión de la seguridad y charlas de concientización.

Nuestro Laboratorio de Análisis de Malware (**LAM**) nos permite ofrecerle una efectiva y rápida solución contra variantes de malware y nuevas amenazas.

Security Labs

eset

COTIZACIÓN - NLEP20161108-42

Producto	Periodo	Precio unt.	Cantidad	Total
ESET Endpoint Antivirus Antivirus y AntiSpyware Detecta y elimina virus, phishing, spyware, adware, rootkits, bots, gusanos troyanos, etc. - Protección para clientes de correo - Consola de Administración. - Servidor de Actualizaciones en red **Soporte técnico**	1 año	S/. 23.20	350	S/. 8,120.00
			Sub Total	S/. 8,120.00
Forma de pago: **15 días** Plazo de entrega: **03 días** Garantía: **01 año**			IGV (18%)	S/. 1,461.60
			Total	**S/. 9,581.60**

Si está de acuerdo con la presente cotización, generar la orden de compra a:

ARCHIVO GENERAL DE LA NACION
Área de Informática

SECURITY LABS PERÚ S.A.C.
RUC 20563462010
AV. GUARDIA CIVIL 864 OF. 401 URB. CORPAC, SAN ISIDRO - LIMA

Si no emite orden de compra, complete los datos y envíe esta hoja firmada a **ventas@securitylabs.pe**

Razón social	RUC
Dirección	
Contacto de pagos	
Correo	Teléfono

Atentamente,

Enrique Palomino Ruidias
Consultor Corporativo
(+51) 987 958 953

09

COMPUTEL S.A.
SOLUCIONES TECNOLÓGICAS PARA SU NEGOCIO

RUC: 20125356517

Lima, 25 de Octubre de 2016

Señores:

COTIZACION 001000-2016-IA

Presente.-

Atención:

Estimados Señores:

Agradeciendo su atención le presentamos nuestra propuesta técnico - económica al mejor costo beneficio.

ITEM	CANT	DESCRIPCION	Nº PARTE	P.U. S/. Incluye IGV	P.T. S/. Incluye IGV	PLAZO ENTREGA
1	350	Mcafee Endpoint Protection Suite	-	S/. 35.17	S/. 12,309.50	**48 HORAS BAJO ORDEN DE COMPRA**

Son:	Doce mil trescientos nueve con 50/100 Soles	**S/. 12,309.50**

PRECIOS INCLUYEN IGV 18%

CONDICIONES COMERCIALES

** PRECIO PUESTO EN LA CIUDAD DE LIMA.

** TIEMPO DE ENTREGA: CONTADOS A PARTIR DE LA CONFORMIDAD DE LA ORDEN DE COMPRA.

** VALIDEZ DE LA OFERTA: 05 DIAS.
** CONDICIONES DE ENTREGA: LOS PRODUCTOS SERAN ENTREGADOS EN SUS OFICINAS / NO INCLUYE SERVICIO DE INSTALACION
** LAS ENTREGAS SOLO EN LIMA METROPOLITANA , LOS ENVIOS A PRODUCTOS PREVIAS
** GARANTIA DEL PRODUCTO: SEGÚN LA MARCA

** EJECUCION DE LA GARANTIA: cubre defectos de fabricación. Garantía queda sin efecto si el daño es debido a fallas eléctricas, actos de vandalismo, acciones o manipulaciones indebidas por personal ajeno a la Empresa. No se aceptaran devoluciones de equipos después de 3 días hábiles de transcurrida la compra. Así mismos los equipos deberán estar sin uso, con empaques y accesorios originales. No se aceptaran cajas rotas. No se acepta devolución de suministros.

CONDICIONES DE ENTREGA

Los productos serán entregados en sus oficinas **NO INCLUYE SERVICIO DE INSTALACIÓN.**
Entregas solo en **LIMA METROPOLITANA MAYORES A $100 DOLARES AMERICANOS**
ENVIOS A PROVINCIA PREVIA COORDINACIÓN..
OBSERVACION ADICIONAL

1. Los productos serán despachados con sus embalajes originales cubiertos solo con Strech Film lo cual podría ocasionar, por una mala manipulación en el transporte, golpes, rasgadura de empaques y/o deterioro grave de los productos que no serán responsabilidad de COMPUTEL S.A.

2. El cliente, si lo considera necesario, debe requerir y aprobar de acuerdo al medio de transporte y destino solicitado, una cotización de un embalaje especial y un seguro de transporte adicional antes del despacho de sus productos.

3. En el caso de que el cliente no solicite o no acepte los costos de embalaje adecuados y del seguro para el transporte de su carga, el riesgo y costo por cualquier incidente (pérdida, deterioro, etc.) será íntegramente de responsabilidad y asumido por el Cliente.

4. La responsabilidad de nuestra empresa termina al momento de entregar el producto con el embalaje solicitado y rotulado en las oficinas de la empresa que transportará el producto.

5. No se aceptan devoluciones, caso contrario el cliente paga un monto adicional por la devolucion o cambio del producto

TÉRMINOS Y FORMA DE PAGO

** FORMA DE PAGO: CONTADO

** CODIGO INTERBANCARIO BBVA CONTINENTAL SOLES N°: 011-384-000100004363 -56

** BCP SOLES N°: 191-1576156-0-66 / BBVA CONTINENTAL SOLES N°: 0011-0384-56-0100004363 / SCOTIABANK SOLES N° 000-0557692
** BCP DOLARES N°: 191-1557992-1-01 / BBVA CONTINENTAL DOLARES N°:0011-0384-59-0100004371 / SCOTIABANK DOLARES N° 000-0216641
Su Orden de Compra debe hacer referencia al presente Nº de cotización en señal de conformidad con las condiciones comerciales.

Atentamente,

Iveth Ambrosio
Consultor Corporativo TIC

Telefono: 433-4066 423-2108 Anexo: 142
iambrosio@computel.com.pe

08

Lima, 31 de octubre de 2016

AGN-00758-2016-MRC

Señores
ARCHIVO GENERAL DE LA NACION
Lima.-

Atención : **Sr. Luis J. Esquivel Torres**

Referencia : **Solución Kaspersky**

De nuestra consideración:

Nos es grato saludarlo a fin de presentarle las soluciones de seguridad informática para la protección global contra virus informáticos, control de dispositivos, protección para dispositivos móviles e intrusiones de Kaspersky.

Kaspersky Endpoint Security for Business es nuestra propuesta de seguridad en la red y del usuario final, donde la protección va más allá del lugar de trabajo para alcanzar a usuarios remotos y a una creciente fuerza de trabajo móvil. En Kaspersky Lab creemos que la libertad y la flexibilidad en las comunicación corporativa es completamente compatible con la protección hermética contra las amenazas a la seguridad de hoy en día, tales como virus y otros programas maliciosos, ataques de hackers, spyware y malware.

Bafing S.A.C. es Partner GOLD certificado de Kaspersky para Perú y ha sido reconocido durante los últimos años como el principal proveedor de soluciones Kaspersky de la región sudamericana.

Bafing reúne conocimiento y experiencia con el objetivo de ofrecer a las empresas peruanas soluciones y soporte técnico proactivo, especializado y personalizado para cada una de sus necesidades en seguridad informática.

Sin otro particular, nos despedimos atentamente;

Richard Concha
Gerente Comercial – División Sistemas

Bafing S.A.C.
Tel +51-12258314 Fax +51-14751128
Av. Del Parque Sur 560 – San Borja – Lima 41 – PERU
RUC: 20199144961
http://www.bafing.com

CARACTERISTICAS BASICAS DE LA SOLUCION PROPUESTA

Kaspersky Endpoint Security Business - Select

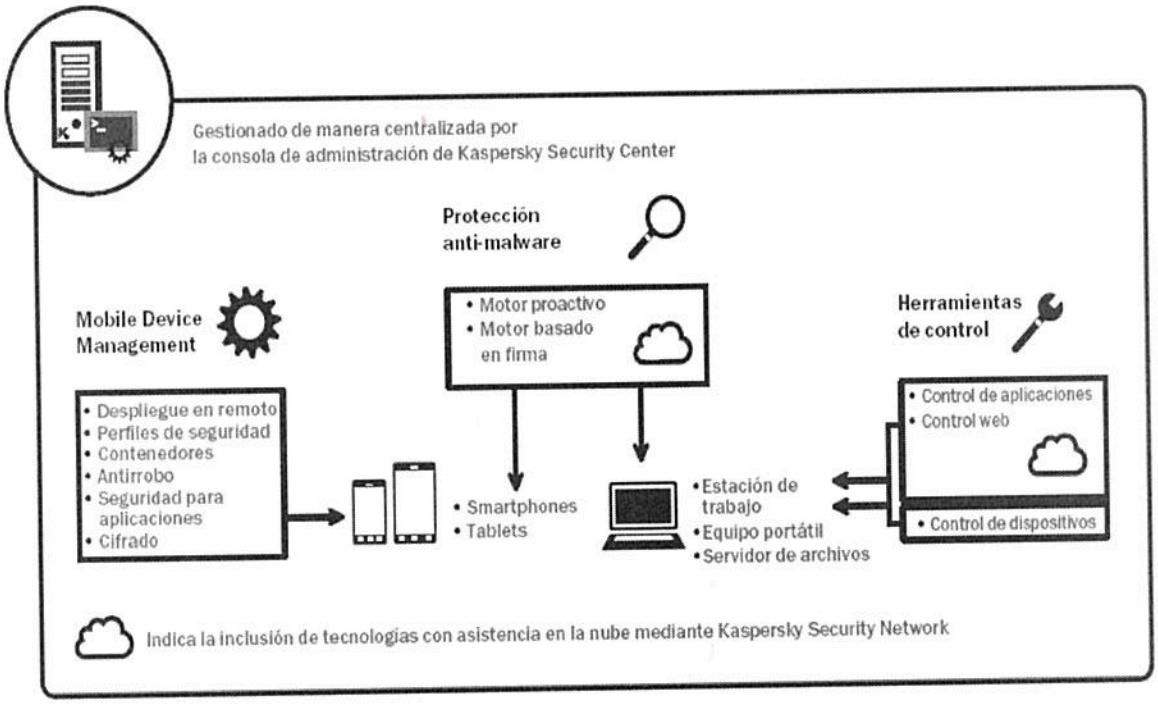
El nivel de protección "Select" de Kaspersky incluye implementación y protección para dispositivos móviles mediante Mobile Device Management (MDM) y funciones anti-malware para móviles. Las herramientas de control de terminales (web, dispositivos y aplicaciones) permiten a tu organización aplicar la política de TI, lo que mantiene seguros los elementos esenciales de tu entorno de TI.

En Kaspersky hemos integrado potentes funciones empresariales en todos los niveles de protección de las soluciones que ofertamos, utilizando siempre una tecnología sencilla e idónea para empresas de cualquier tamaño.

Herramientas para dar soporte a un personal laboral móvil, garantizar el cumplimiento con las políticas de seguridad de TI y bloquear el malware.

Funciones incluidas:

- ANTI-MALWARE
- FIREWALL
- PROTECCIÓN CON ASISTENCIA EN LA NUBE MEDIANTE KASPERSKY SECURITY NETWORK
- CONTROL DE APLICACIONES
- MARCADO DE APLICACIONES EN LISTA BLANCA
- CONTROL WEB
- CONTROL DE DISPOSITIVOS
- PROTECCIÓN DE SERVIDORES DE ARCHIVOS
- MOBILE DEVICE MANAGEMENT
- SEGURIDAD PARA TERMINALES MÓVILES



Bafing S.A.C.
Tel +51-12258314 Fax +51-14751128
Av. Del Parque Sur 560 – San Borja – Lima 41 – PERU
RUC: 20199144961
http://www.bafing.com

PROPUESTA ECONÓMICA

Descripción	Precio Unit.	Cant.	Precio Total
Kaspersky Endpoint Security Business Select ○ Incluye 01 año de Kaspersky Gold Support ○ Instalación de consola de administración Kaspersky Security Center y despliegue de agentes Endpoint Security. ○ Soporte técnico On-Line telefónico, e-mail por 01 año ○ Soporte técnico On-Line Control remoto por 01 año ○ Soporte técnico On-Site por 01 año ○ Capacitación de 06 horas en el manejo, configuración y administración de Kaspersky Security Center y Kaspersky Endpoint Security, hasta 03 personas – se entregará un certificado de asistencia a cada participante	S/ 60.00	350	S/ 21,000.00

COBERTURA DE LA PROPUESTA

Los precios están expresados en Soles
Los precios incluyen el 18% del IGV
Forma de pago: Bafing propone el pago a 15 días de colocada la orden de Compra.
Plazo de entrega: La licencia de software entrega en 10 días calendario.
Vigencia de la propuesta: La presente propuesta tiene una vigencia de 30 días
Presentación del producto: Licencia corporativa de software, múltiples idiomas disponibles.

ARCHIVO GENERAL DE LA NACIÓN
Área de Informática

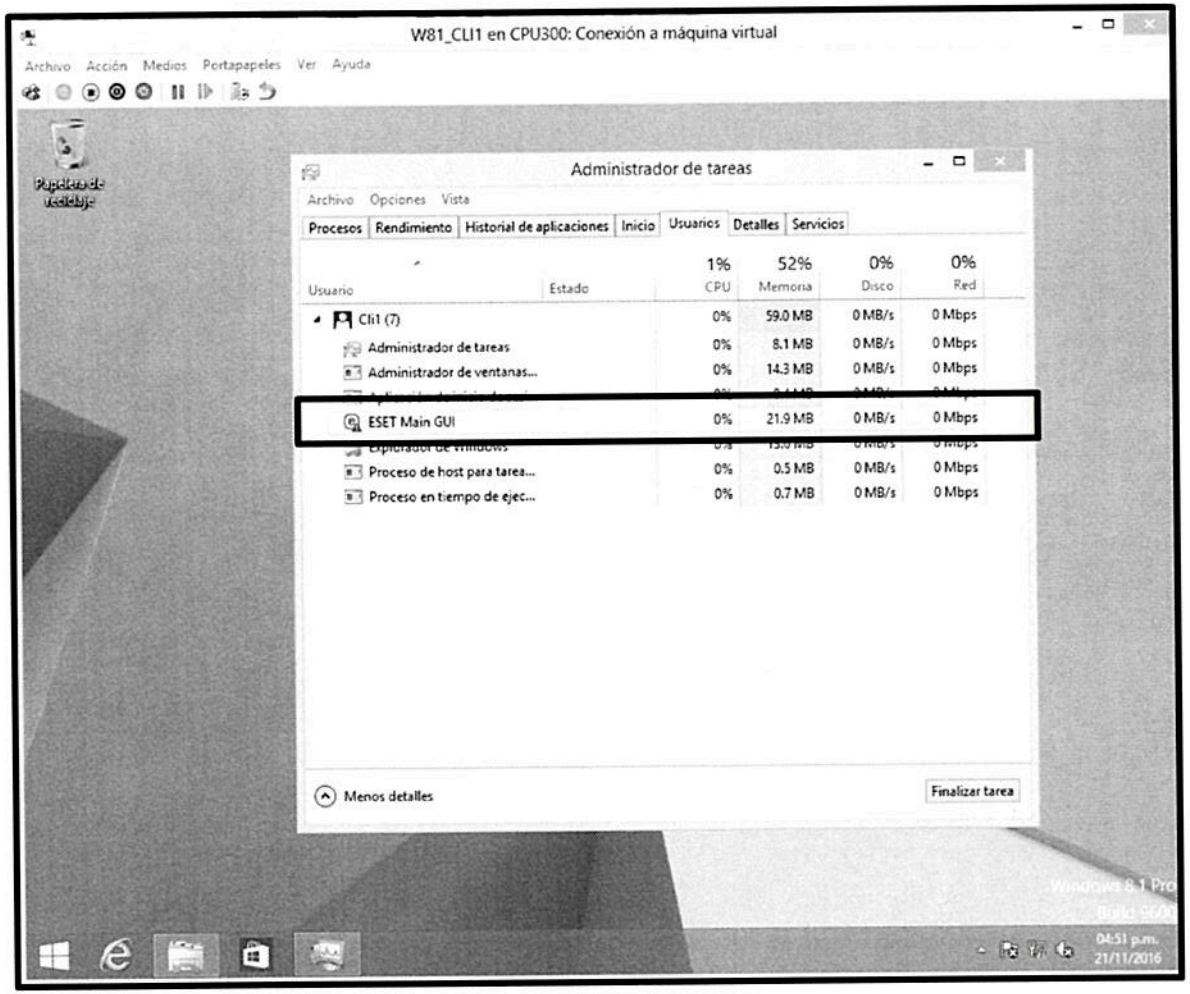
Bafing S.A.C.
Tel +51-12258314 Fax +51-14751128
Av. Del Parque Sur 560 – San Borja – Lima 41 – PERU
RUC: 20199144961
http://www.bafing.com

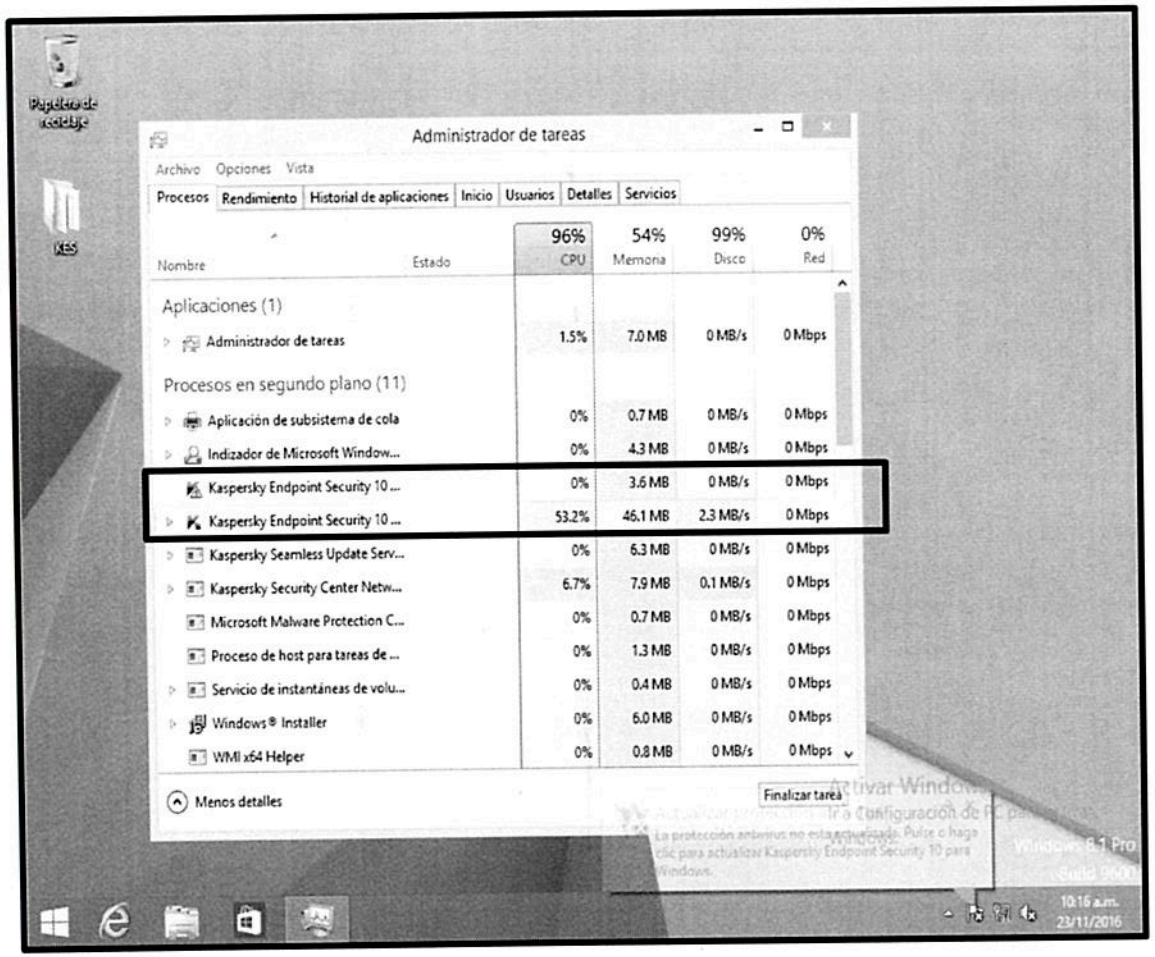
ANEXO 3

ANALISIS COMPARATIVO COSTO BENEFICIO

Eset Endpoint Antivirus

- Fácil de instalar
- Consumo de recursos bajo
- Instalación por paquetes individuales





Kapersky Endpoint Security Bussines

- Fácil de instalar
- Consumo de recursos medio
- Instalación por paquetes grupales

Mcafee Endpoint Protection Suite

- Instalación poco dificultosa
- Consumo de recurso medio
- Instalación por paquetes grupales