



28 DIC. 2016

Judith V. Ruiz Sierra
DIRECTORA

Resolución Jefatural No. 240

-2016-AGN/J

Lima, 28 DIC. 2016

VISTOS, los Informes Técnicos N° 001-2016-AGN/AI y N° 002-2016-AGN/AI-LJET y el Informe Técnico de Estandarización N° 001-2016-AGN/AI del Área de Informática, el Informe N° 355-2016-AGN/OTA-OA de la Oficina de Abastecimiento, el Informe N° 331-2016-AGN/OGAJ y el Memorándum N° 186-2016-AGN/OGAJ de la Oficina General de Asesoría Jurídica, sobre estandarización de la herramienta software antivirus para los equipos de cómputo del Archivo General de la Nación;

CONSIDERANDO:

Que, mediante Informe N° 266-2016-AGN/J-AI, de fecha 28 de noviembre de 2016, el Área de Informática alcanza el Informe Técnico N° 001-2016-AGN/AI, correspondiente a la solicitud de estandarización para la adquisición de la herramienta software antivirus ESET ENDPOINT ANTIVIRUS para los equipos de cómputo del Archivo General de la Nación;

Que, con Informe N° 331-2016-AGN/OGAJ, de fecha 2 de diciembre de 2016, la Oficina General de Asesoría Jurídica señala que, en el Informe Técnico N° 001-2016-AGN/AI, no se ha descrito la verificación de los presupuestos de la estandarización y que tampoco se indican las especificaciones técnicas del bien a contratar; recomendando adecuar el Informe Técnico a las disposiciones de la Directiva N° 004-2016-OSCE/CD "Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular", aprobada por Resolución N° 011-2016-OSCE/PRE y requerir el informe de la Oficina de Abastecimiento, órgano encargado de las contrataciones en el Archivo General de la Nación;

Que, a través del Informe N° 275-2016-AGN/J-AI, de fecha 7 de diciembre de 2016, el Área de Informática remite el Informe Técnico N° 002-2016-AGN/AI-LJET, subsanando las observaciones señaladas por la Oficina General de Asesoría Jurídica;

Que, mediante Informe N° 355-2016-AGN/OTA-OA, de fecha 12 de diciembre de 2016, la Oficina de Abastecimiento considera procedente la estandarización solicitada por el Área de Informática y adjunta el Informe Técnico de Estandarización N° 001-2016-AGN/AI;

Que, el artículo 16 de la Ley N° 30225, Ley de Contrataciones del Estado, establece, en su segundo párrafo, que, salvo las excepciones previstas en el Reglamento, en el requerimiento de contratación "no se hace referencia a una fabricación o una procedencia determinada, o a un procedimiento concreto que caracterice a los bienes o servicios ofrecidos por un proveedor determinado, o a marcas, patentes o tipos, o a un origen o a una producción determinados con la finalidad de favorecer o descartar ciertos proveedores o ciertos productos";

Que, el segundo párrafo del artículo 8 del Reglamento de la Ley N° 30225, aprobado por Decreto Supremo N° 350-2015-EF, establece como supuesto de excepción a la prohibición señalada en el citado artículo 16, el proceso de estandarización debidamente autorizado por el Titular de la Entidad;

Que, la Directiva N° 004-2016-OSCE/CD establece disposiciones específicas y obligatorias en materia de estandarización;

Que, el numeral 7.1 de la Directiva N° 004-2016-OSCE/CD señala que "el área usuaria de la cual proviene el requerimiento de contratar o que, dada su especialidad y funciones, canaliza los requerimientos formulados por otras dependencias, debe elaborar un informe técnico sustentando la necesidad de realizar la estandarización"; asimismo, el numeral 7.2 de la Directiva establece los presupuestos que deben verificarse para que proceda la estandarización, así como los supuestos en que no procede la estandarización;

Que, conforme a lo dispuesto en el numeral 7.3 de la Directiva, el informe técnico referido deberá contener como mínimo lo siguiente: a) La descripción del equipamiento o infraestructura preexistente de la Entidad, b) De ser el caso, la descripción del bien o servicio requerido, indicándose la marca o tipo de producto; así como las especificaciones técnicas o términos de referencia, según corresponda, c) El uso o aplicación que se le dará al bien o servicio requerido, d) La justificación de la estandarización, donde se describa objetivamente los aspectos técnicos, la verificación de los presupuestos de la estandarización antes señalados y la incidencia económica de la contratación, e) Nombre, cargo y firma de la persona responsable de la evaluación que sustenta la estandarización del bien o servicio, y del jefe del área usuaria, y f) La fecha de elaboración del informe técnico;

Que, el Área de Informática sustenta la estandarización en lo siguiente: i) Actualmente el Archivo General de la Nación cuenta con trescientos cincuenta (350) licencias del software ESET ENDPOINT PROTECTION ADVANCED, que operan desde el año 2014; ii) el proceso de estandarización asegurará la compatibilidad en el flujo de información y comunicaciones entre usuarios, garantizará y mantendrá la funcionalidad y operatividad de la infraestructura de software y equipos de cómputo pre existentes en la Entidad; iii) los bienes a adquirir son intangibles y complementarios al equipamiento existente; iv) de la aplicación del modelo de calidad del software, establecido por la Guía de evaluación del software para la administración pública, aprobada por Resolución Ministerial N° 139-2004-PCM, se aprecia que el software ESET ENDPOINT ANTIVIRUS obtiene la más alta puntuación v) el mayor costo para el Archivo General de la Nación al cambiar el software antivirus;

Que, con Memorandum N° 186-2016-AGN/OGAJ, de fecha 21 de diciembre de 2016, la Oficina General de Asesoría Jurídica emite opinión favorable respecto a la estandarización solicitada por el Área de Informática;

Que, conforme a lo solicitado por el Área de Informática el proceso de estandarización será aprobado por el periodo de un (1) año;

Con los visados de la Oficina Técnica Administrativa, la Oficina General de Asesoría Jurídica, la Oficina de Abastecimiento y el Área de Informática;

ARCHIVO GENERAL DE LA NACION
La Dirección de la Oficina de Administración Documentaria, que suscribe, CERTIFICA que esta fotocopia es idéntica a su original que se ha tenido a la vista
Lima,

ARCHIVO GENERAL DE LA NACION
OFICINA DE ADMINISTRACIÓN DOCUMENTARIA
Judith V. Ruiz Sierra
DIRECTORA(e)

28 DIC. 2016



Resolución Jefatural No. 240 -2016-AGN/J

De conformidad con la Ley N° 30225, Ley de Contrataciones del Estado, su Reglamento aprobado por Decreto Supremo N° 350-2015-EF, la Directiva N° 004-2016-OSCE/CD "Lineamientos para la contratación en la que se hace referencia a determinada marca o tipo particular", aprobada por Resolución N° 011-2016-OSCE/PRE, y el Reglamento de Organización y Funciones del Archivo General de la Nación, aprobado por Resolución Ministerial N° 197-93-JUS;

SE RESUELVE:

Artículo Primero.- Aprobar el proceso de estandarización para la adquisición de licencias de software antivirus ESET ENDPOINT ANTIVIRUS, según el detalle del Anexo 1, que forma parte integrante de la presente Resolución.

Artículo Segundo.- Disponer que el proceso de estandarización es aprobado por el periodo de un (1) año.

Artículo Tercero.- Publicar la presente Resolución en el portal web institucional del Archivo General de la Nación (www.agn.gob.pe).

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

ARCHIVO GENERAL DE LA NACIÓN

c. TERESA CARRASCO DE GONZÁLEZ
Jefa Institucional

ARCHIVO GENERAL DE LA NACIÓN
La Dirección de la Oficina de Administración Documentaria, que suscribe, CERTIFICA que esta fotocopia es idéntica a su original que se ha tenido a la vista Lima,

28 DIC. 2016

ARCHIVO GENERAL DE LA NACIÓN
OFICINA DE ADMINISTRACIÓN DOCUMENTARIA

Judith V. Ruiz Sierra
DIRECTORA(E)

Anexo Nro 01

N°	Descripción del bien - ITEM	Cantidad de Licencias
1	Eset Endpoint Antivirus	350

A continuación se detalla las especificaciones técnicas de los bienes requeridos:

Eset Endpoint Antivirus:

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.

PROTECCION 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.

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).



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 ícono 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.




ESPECIFICACIONES DE HARDWARE

Requerimientos del sistema	Procesadores compatibles: Intel® o AMD x86-x64 Sistemas operativos: Microsoft® Windows® 8.1/8/7/Vista/XP/2000 Memoria: 80 MB
ESET Endpoint Antivirus	Espacio en el disco (Descarga): 32-bit: 60 MB; 64-bit: 66 MB Espacio en el disco (Instalación): 32-bit: 76 MB; 64-bit: 90 MB



Requisitos de ESET Remote Administrator	Sistemas operativos: Microsoft Windows 8/7/Vista/XP/2000 Microsoft Windows Server 2012/2008/2003 Navegadores: Internet Explorer® 5.5 y superiores ESET Remote Administrator Server
ESET Remote Administrator Console	Sistemas operativos: Microsoft Windows 8/7/Vista/XP/2000 Microsoft Windows Server 2012/2008/2003



Sin exigencias para sus servidores	ESET Remote Administrator tiene bajos requerimientos de sistema. Por ejemplo, si se instala en un servidor que ejecuta Microsoft Windows Server 2003 y administra 500 instalaciones de clientes, sólo requiere: Procesador de 1 GHz RAM de 1 GB 2 GB de espacio libre en disco Adaptador de red de 100 Mbps
---	---

