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

INFORME TÉCNICO DE ESTANDARIZACION N° 001-2016-AGN/AI

1. NOMBRE DE ÁREA:

- Área de Informática.

2. 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.

3. 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.

4. 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.

ARCHIVO GENERAL DE LA NACION
OFICINA TECNICA ADMINISTRATIVA
OFICINA DE ABASTECIMIENTO
RECIBIDO
12 DIC. 2016
Hora: 05.59. Firma:

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.

5. DESCRIPCION DEL EQUIPAMIENTO DEL ARCHIVO GENERAL DE LA NACION:

El Archivo General de la Nación (AGN) en sus 4 sedes (ExCorreo, Palacio de Justicia, Hawai y Escuela Nacional de Archiveros (ENA) cuentan con equipos de cómputo entre desktops, laptops, servidores, impresoras, NAS y tablets conectados en red y con acceso a internet.

Las sedes se enlazan por una conexión VPN Site to Site permitiendo la comunicación entre sedes y asegurando que si una sede pierde conexión no afecte a la comunicación entre las demás sedes.

6. BIENES A CONTRATAR:

El software ESET Endpoint Antivirus es un bien intangible complementario al equipamiento existente ya que garantizara la funcionabilidad y operatividad de los equipos de cómputo de la institución, mitigando así ataques informáticos que se puedan producir dentro de la sede tales como: virus, malware, spyware, etc., produciendo estos perdida de información, alteración de información, daño de sistema operativo, etc.

Es por ese motivo que se requiere la contratación de este tipo de software.

7. DESCRIPCION DE SOLUCIONES PROPUESTAS

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.

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

8. ANÁLISIS COMPARATIVO TECNICO.

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.

8.1 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**

8.2 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,	3	3	3

		emitiendo alertas cuando estas estén disponibles para su descarga.			
		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 remotamente clientes del antivirus ofertado.	3	3	3
	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**

8.3 ANALISIS COMPARATIVO COSTO BENEFICIO.

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.

9. ESPECIFICACIONES TECNICAS DEL SOFTWARE 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 ***ESET Endpoint Antivirus***	Procesadores compatibles: Intel® o AMD x86-x64 Sistemas operativos: Microsoft® Windows® 8.1/8/7/Vista/XP/2000 Memoria: 80 MB 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 ***ESET Remote Administrator Console***	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 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

10. CRITERIOS TECNICOS:

ESET ENDPOINT ANTIVIRUS: alcanza el nivel de protección contra antivirus, malware, etc. con una atención rápido, dando solución rápida y utilizando pocos recursos para su ejecución.

Se adjunta la sustentación técnica del software ESET ENDPOINT ANTIVIRUS.

11. VIGENCIA DE LA ESTANDARIZACION

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

12. CANTIDAD DE SOFTWARE ANTIVIRUS

350 LICENCIAS

13. LUGAR DE ENTREGA DE LICENCIAS

La entrega de licencias se efectuará en la sede central del AGN.

14. RESPONSABLES DE LA SUPERVISION, COORDINACION, EVALUACION Y CONFORMIDAD

- Avila Goicochea, Vanessa
- Esquivel Torres, Luis Joseph

15. CARGO:

- Administrador y Soporte de Hardware, Software y Redes

16. 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

17. FECHA:

- 12 de diciembre de 2016