



Misión: Prevenir y controlar los accidentes de tránsito, colaborando con los organismos responsables en la reducción de la tasa de mortalidad y morbilidad ocasionada por los mismos, a través de la utilización de medios tecnológicos y la coordinación, promoción, monitoreo y evaluación de las políticas públicas de seguridad vial, dirigidas a todas las personas que circulan por el territorio nacional.

## DICTAMEN TÉCNICO

Asunción, 29 de julio de 2024

**CONVOCATORIA:** LLAMADO ANTSV MCN SERVICIO DE SUSCRIPCIÓN DE SOFTWARE ANTIVIRUS, CON ID N° 444175.

**UOC CONVOCANTE:** AGENCIA NACIONAL DE TRÁNSITO Y SEGURIDAD VIAL.

**UNIDAD O ÁREA REQUIRENTE:** DIRECCIÓN DE INFORMÁTICA – ANTSV.

**FUNCIONARIO O TÉCNICO RESPONSABLE:** LIC. ARTURO RODRÍGUEZ AGUILERA.

**DEPENDENCIA Y CARGO QUE DESEMPEÑA:** DIRECTOR.

### **CONSIDERANDO:**

Lo dispuesto la Resolución DNCP N° 4401/2023, modificado por la Resolución DNCP N° 453/2024 Art. 12 "...a) DICTAMEN TÉCNICO EN EL CUAL SE SUSTENTEN LAS ESPECIFICACIONES TÉCNICAS REQUERIDAS EN EL PROCEDIMIENTO DE CONTRATACIÓN, REFRENDADO POR EL RESPONSABLE DEL ÁREA REQUIRENTE O DEL TÉCNICO QUE LAS RECOMENDÓ.";

**JUSTIFICACIÓN TÉCNICA QUE RESPALDA LA OBJETIVIDAD, IMPARCIALIDAD, REGULARIDAD Y LA RAZONABILIDAD O PROPORCIONALIDAD DE LOS REQUERIMIENTOS TÉCNICOS SOLICITADOS.**

Que, para la presente convocatoria denominado **SERVICIO DE SUSCRIPCIÓN DE SOFTWARE ANTIVIRUS**, el cual la **Dirección de Informática**, identificado en adelante como el área requirente de la convocatoria y especialistas en la determinación de las necesidades a cubrir, han establecido las especificaciones técnicas de forma a cumplir con las **BUENAS PRÁCTICAS DE CIBERSEGURIDAD** establecido en el PLAN NACIONAL DE CIBERSEGURIDAD las cuales incluyen el **USO DE SOFTWARE ANTIVIRUS** con el propósito de proteger al usuario, la confidencialidad, integridad y disponibilidad de su información en línea.


Por ello, la adquisición de licencias de software antivirus es de vital importancia para la protección de los equipos informáticos con los que cuenta la institución, con el objetivo de mitigar posibles vulnerabilidades.

**IDENTIFICAR Y JUSTIFICAR DE FORMA EXPRESA SI ALGÚN REQUERIMIENTO PODRÍA LIMITAR LA PARTICIPACIÓN DE POTENCIALES OFERENTES.**

No aplica.

**SI EN LAS BASES LICITATORIAS SE INDICA UNA MARCA ESPECÍFICA U OTRO DERECHO INTELECTUAL EXCLUSIVO, MENCIONAR LA JUSTIFICACIÓN QUE RESPALDA LO SOLICITADO O QUE NO EXISTE OTRO MODO DE IDENTIFICARLO. SE ACLARA QUE, EN CASO DE INCLUIRLOS, LOS MISMOS TENDRÁN CARÁCTER REFERENCIAL.**

No Aplica.

  
Lic. Arturo Rodríguez Aguilera  
Director de Informática  
ANTSV

Misión: Prevenir y controlar los accidentes de tránsito, colaborando con los organismos responsables en la reducción de la tasa de mortalidad y morbilidad ocasionada por los mismos, a través de la utilización de medios tecnológicos y la coordinación, promoción, monitoreo y evaluación de las políticas públicas de seguridad vial, dirigidas a todas las personas que circulan por el territorio nacional.

SERVICIO SOLICITADO.

ITEM	DESCRIPCION	UNIDAD	CANTIDAD
1	PROVISION DE LICENCIAS ANTIVIRUS – 24 meses	Unidad	70

EXPERIENCIA REQUERIDA

Demostrar la experiencia en provisión de licencias con facturaciones de venta y/o recepciones finales por un monto equivalente al 30 % como mínimo del monto total ofertado en la presente licitación, de cualquiera de los años (2020, 2021, 2022, 2023)

CAPACIDAD TECNICA

El Oferente deberá contar con las siguientes certificaciones y/o requerimientos.

- Certificación ISO 9001/2015 o similar, la similitud debe basarse en los mismos criterios que solicita o certifica la norma ISO 9001/2015 con respecto a la calidad de la gestión de procedimientos de Provisión e integración de bienes y/o servicios.
- El oferente deberá contar con al menos 2 técnicos con certificaciones de la marca ofertada.
- El oferente deberá acreditarse como representante oficial o distribuidor autorizado del software y sus respectivas licencias, según se detalla:
  - El oferente deberá acreditarse como representante oficial o distribuidor autorizado por el fabricante del software ofertado manifestando que posee la capacidad para proveer la cantidad ofertada en el tiempo solicitado. En la misma, deberá constar que se encuentra en condiciones para proveer, instalar, configurar y soportar el software, según lo solicitado en la planilla de especificaciones técnicas, en caso de resultar adjudicatario.

ESPECIFICACIONES TECNICAS

RESUMEN DE BIENES

ITEM	DESCRIPCION	UNIDAD	CANTIDAD
1	PROVISION DE LICENCIAS ANTIVIRUS – 24 meses	Unidad	70

1. PROVICION DE LICENCIAS ANTIVIRUS

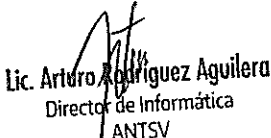
Lic. Arturo Rodríguez Aguilera  
Director de Informática  
ANTSV

Características	Descripción	Exigencia	Cumple / No Cumple
Marca	Especificar	Exigido	
Modelo	Especificar	Exigido	
Procedencia	Especificar	Exigido	
Cantidad	70 (setenta) unidades	Exigido	
Consola de Administración	La administración deberá ser a través de una consola central única, basada en web y en nube, que deberá contener todas las componentes para el monitoreo y control de la protección de los dispositivos	Exigido	

Visión: Ser una institución líder por su excelencia y calidad en la promoción y coordinación de políticas públicas de seguridad vial, orientadas a la prevención y la reducción de los índices de siniestralidad vial.




Misión: Prevenir y controlar los accidentes de tránsito, colaborando con los organismos responsables en la reducción de la tasa de mortalidad y morbilidad ocasionada por los mismos, a través de la utilización de medios tecnológicos y la coordinación, promoción, monitoreo y evaluación de las políticas públicas de seguridad vial, dirigidas a todas las personas que circulan por el territorio nacional.

 <p>Lic. Arturo Rodríguez Aguilera Director de Informática ANTSV</p>	La consola deberá presentar un Dashboard con el resumen del estado de protección de los ordenadores y usuarios, así como indicar las alertas de eventos de criticidades alta, media e informativa	Exigido	
	Debe poseer un mecanismo de comunicación vía API, para su integración con otras soluciones de seguridad, como por ejemplo SIEM	Exigido	
	La consola debe permitir la división de los ordenadores dentro de la estructura de administración en grupos	Exigido	
	Debe permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección.	Exigido	
	Debe poseer la posibilidad de aplicar reglas diferenciadas por grupos de usuarios, usuarios individuales, grupos de máquinas y equipos individuales	Exigido	
	La instalación debe poder realizarse a través del cliente descargado de la consola central y también vía correo electrónico de configuración. El instalador debe permitir la distribución del cliente a través de Active Directory (AD) para múltiples máquinas.	Exigido	
	Proporcionar actualizaciones del producto y de las definiciones de virus y protección contra intrusos	Exigido	
	Debe permitir exclusiones de escaneo para un determinado sitio web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política.	Exigido	
	La consola de administración debe permitir la definición de grupos de usuarios con diferentes niveles de acceso a la configuración, las políticas y los registros	Exigido	
	Actualización incremental, remota y en tiempo real, de las vacunas de los Antivirus y del mecanismo de verificación (Engine) de los clientes	Exigido	
	Permitir la programación de la exploración contra virus con la posibilidad de seleccionar una máquina o grupo de máquinas, con periodicidad definida por el administrador	Exigido	
	Utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los clientes administrados.	Exigido	
	Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.	Exigido	
	Permitir la exportación de los informes gerenciales a los formatos CSV y PDF	Exigido	
	Los recursos del informe y el monitoreo deben ser nativos de la propia consola central de administración	Exigido	
	Posibilidad de mostrar información como nombre de la máquina, versión del antivirus, sistema operativo, dirección IP, versión del motor, fecha de la actualización, fecha de la última verificación, eventos recientes y estado	Exigido	
	La comunicación debe permitir QoS para controlar el ancho de banda de red.	Exigido	


Visión: Ser una institución líder por su excelencia y calidad en la promoción y coordinación de políticas públicas de seguridad vial, orientadas a la prevención y la reducción de los índices de siniestralidad vial.

Misión: Prevenir y controlar los accidentes de tránsito, colaborando con los organismos responsables en la reducción de la tasa de mortalidad y morbilidad ocasionada por los mismos, a través de la utilización de medios tecnológicos y la coordinación, promoción, monitoreo y evaluación de las políticas públicas de seguridad vial, dirigidas a todas las personas que circulan por el territorio nacional.

	Debe permitir seleccionar un grupo de equipos para aplicar la actualización para controlar el ancho de banda de red. La actualización de la versión debe ser transparente para los usuarios finales.	Exigido	
	La herramienta de administración centralizada debe administrar todos los componentes de la protección para estaciones de y debe diseñarse para administrar, supervisar y elaborar informes de endpoint.	Exigido	
	La Consola de administración debe incluir un panel con un resumen visual en tiempo real para comprobar el estado de seguridad	Exigido	
	Deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los ordenadores que necesitan atención	Exigido	
	Deberá mostrar los ordenadores administrados de acuerdo con los criterios de categoría (detalles del estado del equipo, detalles sobre la actualización, detalles de avisos y errores, detalles del antivirus, etc.), y ordenar los equipos en consecuencia	Exigido	
	Actualizar de forma automática las directivas de seguridad cuando un equipo se mueve de un grupo a otro	Exigido	
	Grabar un registro de auditoría seguro que supervise la actividad en la consola de administración para el cumplimiento de regulaciones, auditorías de seguridad, análisis y solución de problemas forenses	Exigido	
	Deberá permitir exportar el informe de registros de auditoría en formatos CSV y PDF	Exigido	
	Debe contener varios informes para el análisis y control de los usuarios y endpoints. Los informes se deben dividir, como mínimo, en informes de: eventos, usuarios, control de aplicaciones, periféricos y web, indicando todas las funciones solicitadas para los endpoints	Exigido	
	Permitir la ejecución manual de todos estos informes, así como la programación y envío automático por correo electrónico en los formatos CSV y PDF	Exigido	
<div>Capacidad de generación de informes</div> <div><div>Lic. Arturo Rodríguez Aguilera Director de Informática ANTSV</div></div>	Debe realizar envío automático de alertas críticas mediante correo electrónico a los administradores	Exigido	
	Detalle de usuarios activos, inactivos o desprotegidos, así como detalles de los mismos	Exigido	
	Detalle de los ordenadores que están activos, inactivos o desprotegidos, así como detalles de las exploraciones y alertas en los ordenadores	Exigido	
	Detalle de los periféricos permitidos o bloqueados, así como detalles de dónde y cuándo se utilizó cada periférico	Exigido	
	Detalle de las principales aplicaciones bloqueadas y los servidores / usuarios que intentaron acceder a ellas	Exigido	
	Detalle de las aplicaciones permitidas que fueron accedidas con mayor frecuencia y los servidores / usuarios que las acceden	Exigido	
	Detalle de los servidores / usuarios que intentaron acceder a aplicaciones bloqueadas con mayor frecuencia y las aplicaciones que ellos intentaron acceder	Exigido	


Visión: Ser una Institución líder por su excelencia y calidad en la promoción y coordinación de políticas públicas de seguridad vial, orientadas a la prevención y la reducción de los índices de siniestralidad vial.

Misión: Prevenir y controlar los accidentes de tránsito, colaborando con los organismos responsables en la reducción de la tasa de mortalidad y morbilidad ocasionada por los mismos, a través de la utilización de medios tecnológicos y la coordinación, promoción, monitoreo y evaluación de las políticas públicas de seguridad vial, dirigidas a todas las personas que circulan por el territorio nacional.

	Detalle de todas las actividades disparadas por reglas de fuga de información.	Exigido	
Idiomas	Inglés (predeterminado)	Exigido	
	Portugués	Exigido	
	Alemán	Exigido	
	Francés	Exigido	
	Italiano	Exigido	
	Español	Exigido	
	Japonés	Exigido	
	Chino (tradicional y simplificado)	Exigido	
Opciones de corrección de problemas	Proteger el dispositivo con la opción de inicio de una exploración	Exigido	
	Forzar una actualización en ese momento	Exigido	
	Ver los detalles de los eventos ocurridos	Exigido	
	Ejecutar la comprobación completa del sistema	Exigido	
	Forzar el cumplimiento de una nueva política de seguridad	Exigido	
	Mover el equipo a otro grupo	Exigido	
	Borrar el equipo de la lista	Exigido	
Características básicas del agente de protección	El agente antivirus debe proteger computadoras portátiles, escritorios y servidores en tiempo real, bajo demanda o programado para detectar, bloquear y limpiar todos los virus, troyanos, gusanos y spyware. En Windows, el agente también debe detectar PUA, adware y comportamiento sospechoso,	Exigido	
	Además del control de amenazas, el mismo agente (al menos Windows) debe proporcionar control de dispositivos, control de aplicaciones, control web y prevención de fuga de información (DLP).	Exigido	
	Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido	Exigido	
	Debe realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque	Exigido	
	Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA)	Exigido	
	Debe proteger las funciones críticas en los navegadores de Internet (Safe Browsing)	Exigido	
	Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos	Exigido	
	Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo virus, spyware, troyanos, gusanos, adware y aplicaciones potencialmente no deseadas (PUA)	Exigido	
<div><div>Lic. Arturo Rodríguez Aguilera Director de Informática ANTSV</div></div>	Posee la funcionalidad de protección contra el cambio de la configuración del agente, impidiendo a los usuarios, incluyendo el administrador local, reconfigurar, deshabilitar o desinstalar componentes de la solución de protección	Exigido	


Visión: Ser una institución líder por su excelencia y calidad en la promoción y coordinación de políticas públicas de seguridad vial, orientadas a la prevención y la reducción de los índices de siniestralidad vial.

Misión: Prevenir y controlar los accidentes de tránsito, colaborando con los organismos responsables en la reducción de la tasa de mortalidad y morbilidad ocasionada por los mismos, a través de la utilización de medios tecnológicos y la coordinación, promoción, monitoreo y evaluación de las políticas públicas de seguridad vial, dirigidas a todas las personas que circulan por el territorio nacional.

<div><div>Lic. Arturo Rodríguez Aguilera Director de Informática ANTSV</div></div>	Debe tener un mecanismo contra la desinstalación del endpoint por el usuario y cada dispositivo deberá tener una contraseña única, no siendo autorizadas soluciones con una contraseña que funcione en todos los dispositivos	Exigido	
	Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de los componentes de protección	Exigido	
	Ser capaz de aplicar un análisis adicional, inspeccionando finamente el comportamiento de los códigos durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.	Exigido	
	Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits	Exigido	
	Debe permitir el monitoreo y el control de dispositivos extraíbles en los equipos de los usuarios, como dispositivos USB, periféricos de la propia estación de trabajo y redes inalámbricas, aplicando estas políticas tanto para usuarios como para dispositivo	Exigido	
	El control de dispositivos debe estar al nivel de permiso, sólo lectura o bloqueo	Exigido	
	Los siguientes dispositivos deben ser, como mínimo, administrados: HD (hard disks) externos, pendrives USB, almacenables removibles seguras, CD, DVD, Blu-ray, floppy drives, interfaces de red inalámbrica, módems, bluetooth, infrarrojo, MTP (Media Transfer Protocol) y PTP (Picture Transfer Protocol) como cámaras digitales	Exigido	
	Control de aplicaciones para monitorear e impedir que los usuarios ejecuten o instalen aplicaciones que puedan afectar la productividad o el rendimiento de la red	Exigido	
	Capacidad de reconocer y bloquear automáticamente las aplicaciones en los clientes basándose en la huella digital (hash) del archivo.	Exigido	
	Actualización automática de la lista de aplicaciones que se pueden controlar, permitiendo aplicaciones específicas o las categorías específicas de aplicaciones que pueden ser liberadas o bloqueadas	Exigido	
	Detectar aplicaciones controladas cuando los usuarios acceden, con las opciones de permitir y alertar o bloquear y alertar	Exigido	
	Debe contar con prevención de intrusión en el host (HIPS), que monitoree el código y bloques de código que pueden comportarse de forma maliciosa antes de ser ejecutados	Exigido	
	Control de acceso a sitios web por categoría	Exigido	
	El Control Web debe controlar el acceso a sitios inapropiados, con al menos 14 categorías de sitios inadecuados. También debe permitir la creación de listas blancas y listas negras.	Exigido	
	La aplicación de políticas de control web, debe contar con capacidad de horarios.	Exigido	

Misión: Prevenir y controlar los accidentes de tránsito, colaborando con los organismos responsables en la reducción de la tasa de mortalidad y morbilidad ocasionada por los mismos, a través de la utilización de medios tecnológicos y la coordinación, promoción, monitoreo y evaluación de las políticas públicas de seguridad vial, dirigidas a todas las personas que circulan por el territorio nacional.

	Debe poseer protección de fugas o pérdida de datos sensibles en el mismo agente de protección, considerando su contenido, además de la posibilidad de evaluar la extensión del archivo y múltiples destinos	Exigido	
	Permitir la identificación de información confidencial, como números de pasaporte u otra información personal identificable y / o información confidencial, incluso si los documentos no se han clasificado correctamente, utilizando CCL (Lista de control de contenido)	Exigido	
	Posibilitar el bloqueo, sólo registrar el evento en la Consola de administración, o preguntar al usuario si él o ella realmente quiere transferir el archivo identificado como sensible	Exigido	
	Soportar agregar reglas propias de contenido con un asistente proporcionado para este propósito	Exigido	
	Capacidad de autorizar, bloquear y confirmar el movimiento de información sensible y en todos los casos, grabar la operación realizada con las principales informaciones de la operación	Exigido	
	El Agente para servidores debe contemplar monitoreo de integridad de archivos, al menos en servidores Windows.	Exigido	
Identificadores de listas CCL preconfiguradas	Números de tarjetas de crédito	Exigido	
	Números de cuentas bancarias	Exigido	
	Números de pasaportes	Exigido	
	Direcciones	Exigido	
	Números de teléfono	Exigido	
	Lista de correos electrónicos	Exigido	
Medios para control de datos	Adjunto en el cliente de correo electrónico (al menos Outlook y Outlook Express)	Exigido	
	Adjunto en el navegador (al menos IE, Firefox y Chrome)	Exigido	
	Adjunto en el cliente de mensajería instantánea (al menos Skype)	Exigido	
	Adjunto a dispositivos de almacenamiento (al menos USB, CD / DVD)	Exigido	
Funcionalidad de detección proactiva de reconocimiento de nuevas amenazas	Protección de amenazas de día 0 a través de tecnología de deep learning (signature less).	Exigido	
	Funcionalidad de detección de amenazas desconocidas que están en memoria	Exigido	
	Capacidad de detección, y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria	Exigido	
	Capacidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria	Exigido	
	No debe requerir descarga de firmas de ningún tipo.	Exigido	
	Capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.	Exigido	



Lic. Ariuro Rodríguez Aguilera

Director de Informática

ANTSV



Misión: Prevenir y controlar los accidentes de tránsito, colaborando con los organismos responsables en la reducción de la tasa de mortalidad y morbilidad ocasionada por los mismos, a través de la utilización de medios tecnológicos y la coordinación, promoción, monitoreo y evaluación de las políticas públicas de seguridad vial, dirigidas a todas las personas que circulan por el territorio nacional.


	Análisis forense de lo sucedido, para entender cuál fue la causa raíz del problema con el detalle de los procesos y sub-procesos ejecutados, la lectura y escritura de archivos y de las claves de registro.	Exigido	
	Bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).	Exigido	
	Generación de excepciones ante falsos positivos.	Exigido	
Funcionalidad de protección contra ransomware	Disponer de capacidad de protección contra ransomware basada en comportamiento	Exigido	
	Disponer de capacidad de remediación de la acción de encriptación de los ransomware	Exigido	
	Capacidad de detección del cifrado malicioso de forma local o remoto	Exigido	
	Debe poseer protección anti-ransomware para el sector de booteo (master boot record).	Exigido	
	Debe restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.	Exigido	
	Debe informar a la consola todo el detalle del incidente – análisis de causa raíz sin la necesidad de instalar otro agente o dispositivo en la red.	Exigido	
Protección contra Vulnerabilidades y técnicas de explotación	Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidades conocidas o de día cero	Exigido	
	Mitigación de inyección de códigos en procesos	Exigido	
	Protección contra robo de credenciales	Exigido	
	Protección contra malware escondido en aplicaciones legítimas (code cave)	Exigido	
	Evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.	Exigido	
	Evitar obtener escalamiento de privilegios	Exigido	
	Modificación de las claves de registro para la ejecución de código arbitrario	Exigido	
Detección y protección de las siguientes técnicas de explotación	Enforce Data Execution Prevention	Exigido	
	Mandatory Address Space Layout Randomization	Exigido	
	Bottom-up ASLR	Exigido	
	Null Page (Null Deference Protection)	Exigido	
	Heap Spray Allocation	Exigido	
	Dynamic Heap Spray	Exigido	
	Stack Pivot	Exigido	
	Stack Exec (MemProt)	Exigido	
	Stack-based ROP Mitigations (Caller)	Exigido	
	Branch-based ROP Mitigations (Hardware Assisted)	Exigido	
	Structured Exception Handler Overwrite (SEHOP)	Exigido	
	Import Address Table Filtering (IAF)	Exigido	
	Load Library	Exigido	
	Reflective DLL Injection	Exigido	
	Shellcode	Exigido	

  
Lic. Arturo Rodríguez Aguilera  
Director de Informática  
ANTSV

Visión: Ser una institución líder por su excelencia y calidad en la promoción y coordinación de políticas públicas de seguridad vial, orientadas a la prevención y la reducción de los índices de siniestralidad vial.

Misión: Prevenir y controlar los accidentes de tránsito, colaborando con los organismos responsables en la reducción de la tasa de mortalidad y morbilidad ocasionada por los mismos, a través de la utilización de medios tecnológicos y la coordinación, promoción, monitoreo y evaluación de las políticas públicas de seguridad vial, dirigidas a todas las personas que circulan por el territorio nacional.

	VBScript God Mode	Exigido	
	Wow64	Exigido	
	Syscall	Exigido	
	Hollow Process	Exigido	
	DLL Hijacking	Exigido	
	Squiblydoo Applocker Bypass	Exigido	
	APC Protection (Double Pulsar / AtomBombing)	Exigido	
	Process Privilege Escalation	Exigido	
Despliegue Agente	Soportar máquinas con arquitectura de 32 bits y 64 bits	Exigido	
	El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Mac OS X 10.10 en adelante,	Exigido	
	El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Windows 7 en adelante	Exigido	
	El cliente para instalación en servidores debe ser compatible con los sistemas operativos Windows server 2008 en adelante.	Exigido	
Sistemas Operativos Linux soportados (en tiempo real)	CentOS 6/7	Exigido	
	Debian 9	Exigido	
	Oracle Linux 6/7	Exigido	
	Red Hat Enterprise Linux 6/7	Exigido	
	SUSE 12/15	Exigido	
	Ubuntu 14/16/18	Exigido	
Vigencia	24 meses	Exigido	
Soporte	Deberá incluir 70 horas de servicio de soporte in situ o remoto por parte del oferente adjudicado, durante el periodo de vigencia de las licencias.	Exigido	
Autorización	El oferente deberá contar con una autorización apostillada del fabricante para presentar la oferta. A su vez, el oferente deberá estar debidamente autorizado por el fabricante para prestar servicio técnico.	Exigido	



Lic. Arturo Rodríguez Aguilera

Director de Informática

ANTSV



AGENCIA NACIONAL DE  
**TRÁNSITO Y  
SEGURIDAD VIAL**  
PARAGUAY

PARAGUÁI  
**TETÁ RAPE  
JEPORUKUAAHA**  
TEKOVE ÑANGAREKORÁ RENDA

**Misión:** Prevenir y controlar los accidentes de tránsito, colaborando con los organismos responsables en la reducción de la tasa de mortalidad y morbilidad ocasionada por los mismos, a través de la utilización de medios tecnológicos y la coordinación, promoción, monitoreo y evaluación de las políticas públicas de seguridad vial, dirigidas a todas las personas que circulan por el territorio nacional.

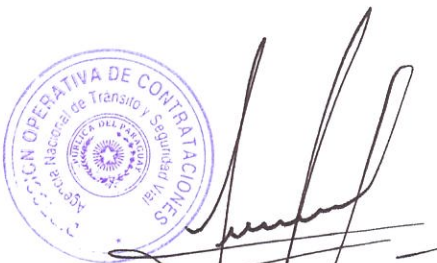
### **CONCLUSIÓN:**

Por todo lo expuesto anteriormente, respecto a el proceso de contratación denominado "**SERVICIO DE SUSCRIPCIÓN DE SOFTWARE ANTIVIRUS**", cabe destacar que dichas especificaciones se realizaron de manera a contar con un software antivirus capaz de cumplir con las características esenciales para garantizar la seguridad de los equipos tecnológicos de la Institución, en ese sentido se emite el presente dictamen técnico, considerando haber cumplido con las disposiciones de la DNCP, con relación al mecanismo para la obtención de las Especificaciones Técnicas, estos criterios son esenciales para garantizar un proceso de contratación público justo, eficiente y que cumpla con los estándares de calidad requeridos.



**Lic. Arturo Rodríguez Aguilera**, Director  
Dirección de Informática

Agencia Nacional de Tránsito y Seguridad Vial



**Lic. Fabian Candia Riveros**, Director  
Dirección Operativa de Contrataciones  
Agencia Nacional de Tránsito y Seguridad Vial

**Visión:** Ser una institución líder por su excelencia y calidad en la promoción y coordinación de políticas públicas de seguridad vial, orientadas a la prevención y la reducción de los índices de siniestralidad vial.