



Poder Judicial de la Ciudad Autónoma de Buenos Aires

Ministerio Público Tutelar

Departamento de Tecnología y Comunicaciones

"2018 Año de los Juegos Olímpicos de la Juventud"

## ANEXO III

### PLIEGO DE ESPECIFICACIONES TÉCNICAS

#### 1. Características Generales

1.1 El presente llamado tiene por objeto la renovación y actualización de las licencias de software del producto antivirus denominado comercialmente ESET EndPoint Protection, 325 licencias antivirus para estaciones de trabajo y servidores, 15 licencias para notebooks y la adquisición de 65 licencias para nuevas estaciones de trabajo y servidores, por el término de 24 meses, actualmente desplegada en el Ministerio Público Tutelar.

#### 2. Descripción del software

2.1 Antivirus ESET EndPoint Protection Standard para 390 estaciones de trabajo y servidores.

2.2 Antivirus ESET EndPoint Protection Advanced para 15 notebooks.

#### 3. Consideraciones técnicas

3.1

Servidor/es		Estaciones Cliente	
Sistema Operativo	Cantidad	Sistema Operativo	Cantidad
Linux	10	Windows 10	350
Windows	30	-	-
Subtotal	40	Subtotal	350
<b>Total ESET ENDPoint Protection Standard: 390 licencias</b>			

48



Ministerio Público Tutelar  
Poder Judicial de la Ciudad de Buenos Aires

### 3.2

Notebooks	
Sistema Operativo	Cantidad
Windows 10	15
Subtotal	15
<b>Total ESET ENDPoint Protection Advanced: 15 licencias</b>	

## 4. Características técnicas del equipamiento

### 4.1

Servidores			Estaciones Cliente			Notebooks		
Procesador	Memoria	Espacio en disco	Procesador	Memoria	Espacio en disco	Procesador	Memoria	Espacio en disco
Intel Xeon E5-2603	16 GB	8 TB	Intel Core i5	4 GB	500 GB	Intel Core i7	8 GB	320 GB
Intel Xeon E5-2620	64 GB	5,5 TB	Intel Core i5	8 GB	500 GB	-	-	-
Intel Xeon X5570	16 GB	160 GB	-	-	-	-	-	-

Se deberá garantizar el correcto funcionamiento del software en base a las características técnicas mencionadas.

## 5. Instalación y actualización de licencias

5.1 Soporte de instalación centralizada (desatendida por parte del usuario de la PC). El administrador podrá programar la actualización de los equipos seleccionando:

- Todas las estaciones de trabajo.
- Un grupo de estaciones de trabajo.



---

**Poder Judicial** de la Ciudad Autónoma de Buenos Aires

---

**Ministerio Público Tutelar**

---

Departamento de Tecnología y Comunicaciones

---

"2018 Año de los Juegos Olímpicos de la Juventud"

---

## 5.2 Soporte de actualización "en-línea" y manual.

Soporte de programación de actualizaciones hacia todos los clientes y servidores en modo:

- Centralizado.
- Automático.

## 6. Tecnología y características del software

6.1 La solución deberá poder realizar exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso.

Debe tener un control web para limitar el acceso a los sitios web por categoría o bien una categoría de sitios web, además de mostrar al usuario una notificación de bloqueo.

Capacidad para instalar los parches del sistema operativo compatible Windows 10 y 7.

La solución de antivirus debe ejecutar un escaneo o exploración de cualquiera de los siguientes estados en la computadora:

- Protector de pantalla o salvapantallas activo
- Sesión de usuario bloqueada
- Sesión de usuario finalizada

La solución deberá contar por lo menos con las siguientes opciones de exploración.

- Exploración Inteligente
- Exploración personalizada
- Exploración de medios removibles
- Repetir última exploración



**Ministerio Público Tutelar**

Poder Judicial de la Ciudad de Buenos Aires

---

Perú 143, 10° piso. (CP 1079) Tel.: 5297-8000 · agt@jusbaire.gob.ar · www.mptutelar.gob.ar

---

Detección y eliminación de virus conocidos y desconocidos en las estaciones cliente y/o servidores según el método de rastreo seleccionado (tiempo real, demanda, programado, etc.):

- Virus de arranque
- Virus de archivos
- Virus Macros
- Virus de VB scrip y Java Script
- Virus en archivos compactados
- Virus en archivos compactados en distintos niveles
- Reconocimiento de "firmas de virus"
- Reconocimiento Heurístico
- Rasonware

Chequeo automático de la transferencia de archivos entre clientes y servidores.

Rastreo de infecciones en un registro de actividad.

Soporte de antispyware.

Soporte para la prevención de ingreso de virus a través de Mensajería Instantánea:

- SKYPE

Soporte para la prevención de ingreso de virus a través de Correo electrónico:

- POP3
- IMAP

El producto deberá tener una sólida trayectoria de confiabilidad a través del tiempo. A tales efectos se requiere que el producto haya sido sometido a todas las auditorías realizadas por Virus Bulletin ([www.virusbtn.com](http://www.virusbtn.com)) en los últimos 12 meses, sin tener falla en la detección de los virus "in the wild" y sin haber emitido ningún falso positivo.

Debe haber obtenido la certificación Advanced+ en todas las evaluaciones retrospectivas del 2007 hechas por AV-Comparative.org que garantizan el desempeño de los productos antivirus en cuanto a protección contra nuevos virus en forma heurística con bajas tasas de falsos positivos.

Ejecutarse en equipos PC con mínimo impacto en el rendimiento del equipo, no debiendo producir una degradación superior al 20%

Contar con no más de 2 procesos activos en memoria a fin de que el producto consuma la menor cantidad de recursos del sistema.

## **7. Características de la consola**

7.1 Deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados a través de la consola, de terceros.



---

**Poder Judicial de la Ciudad Autónoma de Buenos Aires**

---

**Ministerio Público Tutelar**

---

**Departamento de Tecnología y Comunicaciones**

---

"2018 Año de los Juegos Olímpicos de la Juventud"

---

Debe permitir generar grupos de clientes dinámicos y grupos estáticos.

El fabricante debe proporcionar al menos tres diferentes formas de realizar la instalación de la consola de administración.

- Instalador todo en uno
- Instalación por componentes
- Aparato virtual

El aparato virtual debe soportar al menos las siguientes plataformas de virtualización:

- VMWare vSphere
- Oracle Virtual Box
- Microsoft Hyper-V
- Azure - ambiente basado en la nube

La consola de Administración deberá soportar su instalación sobre Linux.

Deberá tener una consola de administración de licencias en la nube, donde se pueda revisar el detalle de los equipos a los que se les ha provisionado licenciamiento.

Activar el acceso a la consola de antivirus con doble factor de autenticación, deber estar integrada a la misma consola de antivirus, sin ningún add-on ó software adicional.

La solución debe tener el mecanismo para quitar otras soluciones antivirus presentes en el endpoint. Este mecanismo debe ser o estar:

- Integrado a la solución antivirus
- Como una herramienta independiente
- Disponible solamente a través de una consola de administración

El servidor deberá contar con un módulo MDM que permite la conexión y gestión de los dispositivos móviles dentro de la red.



---

**Ministerio Público Tutelar**  
Poder Judicial de la Ciudad de Buenos Aires

---

Perú 143, 10º piso. (CP 1079) Tel.: 5297-8000 · agt@jusbares.gob.ar · [www.mptutelar.gob.ar](http://www.mptutelar.gob.ar)

---

A través de la consola, deberá posibilitar la instalación y desinstalación de software de terceros, no sólo de las soluciones de seguridad.

La consola de administración deberá permitir definir un desencadenador para ejecutar una acción predeterminada ante un suceso que pudiera ocurrir dentro de la red.

## **8. Del fabricante**

8.1 El fabricante deberá tener soporte técnico en castellano, así como también, tener documentación publicada en internet en castellano.

Deberá directamente brindar servicios de seguridad informática como por ejemplo penetration testing, vulnerability assessment o análisis de GAP.

Deberá tener un laboratorio de análisis y detección de malware en Latinoamérica, oficinas de la marca en Latinoamérica y presencia local en el país.

## **9. Entrega del producto**

9.1 La entrega del producto deberá realizarse a partir del día 28 de junio de 2018, o vencida esta fecha a partir de su adjudicación según Pliego de Bases y Condiciones Particulares. La misma, podrá realizarse a través de un correo electrónico en el cual se detallen los datos de las licencias solicitadas y URL con la descarga del producto, el cual deberá ser enviado a [dtc-mpt@jusbaire.gob.ar](mailto:dtc-mpt@jusbaire.gob.ar).



Dr. Gustavo Javier Terriles  
Director de Programación y Control  
Presupuesto y Contable  
MINISTERIO PÚBLICO TUTELAR



Poder Judicial de la Ciudad Autónoma de Buenos Aires

Ministerio Público Tutelar

Departamento de Tecnología y Comunicaciones

"2018 Año de los Juegos Olímpicos de la Juventud"

#### ANEXO IV

#### DETALLE ESPECIFICACIONES TÉCNICAS

Renglón	Detalle	Cantidad
1	Licencias ESET EndPoint Protection Standard	390
2	Licencias ESET EndPoint Protection Advanced	15

  
Dr. Gustavo Javier Terriles  
Director de Programación y Control  
Presupuesto y Contable  
MINISTERIO PÚBLICO TUTELAR



Ministerio Público Tutelar  
Poder Judicial de la Ciudad de Buenos Aires

