

Guía de Seguridad de las TIC CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC - Anexo B.1: Herramientas anti-virus/EPP



Noviembre 2017

Edita:



© Centro Criptológico Nacional, 2017

NIPO: 785-17-037-2.

Fecha de Edición: noviembre 2017

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN Y OBJETO	4
2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS	5
2.1 FUNCIONALIDAD	5
2.2 CASOS DE USO.....	5
2.2.1. CASO DE USO 1- GESTIÓN CENTRALIZADA.....	5
2.2.2. CASO DE USO 2 - GESTIÓN INDIVIDUALIZADA	5
2.3 ENTORNO DE USO	6
2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO	6
2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)	6
3. ANÁLISIS DE AMENAZAS	8
3.1 RECURSOS QUE ES NECESARIO PROTEGER.....	8
3.2 AMENAZAS	8
4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS).....	9
4.1 PERFIL DE PROTECCIÓN	9
4.2 REQUISITOS CRIPTOGRÁFICOS.....	9
4.3 REGISTROS AUDITORIA	9
4.4 IDENTIFICACIÓN Y AUTENTICACIÓN	10
4.5 VIRUS.....	10
5. ABREVIATURAS.....	12

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Herramientas Anti-virus/EPP (Endpoint Protection Platform)** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), publicado por el CCN.
2. Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia debe implementar para un determinado caso de uso, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza y considerarse objetivamente cualificado desde el punto de vista de la seguridad para ser empleado en los sistemas de información del sector público a las que sea de aplicación el Esquema Nacional de Seguridad (ENS). Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.
3. Además, la aplicación de estos criterios permitirá:
 - Que se establezcan unas características mínimas de seguridad que sirvan de referencia a los **fabricantes** a la hora de desarrollar nuevos productos STIC.
 - Que los **organismos responsables de la adquisición** dispongan de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrecen dichos productos.
 - Que los **usuarios finales** posean una guía que facilite el despliegue y garantice el uso apropiado del producto desde el punto de vista de la seguridad.
4. Por lo tanto, los productos catalogados dentro de la familia **Herramientas Anti-virus/EPP (Endpoint Protection Platform)** conforme a la taxonomía definida por el Centro Criptológico Nacional, serán susceptibles de ser evaluados usando como referencia este documento.
5. En el caso de productos multipropósito, queda fuera del alcance de este documento cualquier otra funcionalidad de seguridad proporcionada, más allá de la especificada para esta familia en la sección siguiente. Dichos productos podrían optar a ser incluidos de manera adicional como Productos Cualificados en otra(s) familia(s) del CPSTIC si cumpliesen los RFS correspondientes.

2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS

2.1 FUNCIONALIDAD

6. Las herramientas *Anti-virus/EPP* son aplicaciones software diseñadas para la prevención, detección y desinfección de virus informáticos.
7. Los virus informáticos son partes de código de una aplicación software que tienen una finalidad dañina. Típicamente está diseñado para replicarse y extenderse dentro de un sistema informático.

2.2 CASOS DE USO

8. Dependiendo de las funcionalidades del producto explotadas y de la finalidad o el contexto en que se utilicen, se contemplan dos casos de uso para esta familia de productos tal y como se definen a continuación.

2.2.1. CASO DE USO 1- GESTIÓN CENTRALIZADA

9. Se realiza una gestión centralizada, que permite monitorizar y controlar la ejecución de varias instancias de la aplicación de antivirus que se ejecuta sobre un grupo heterogéneo de sistemas.

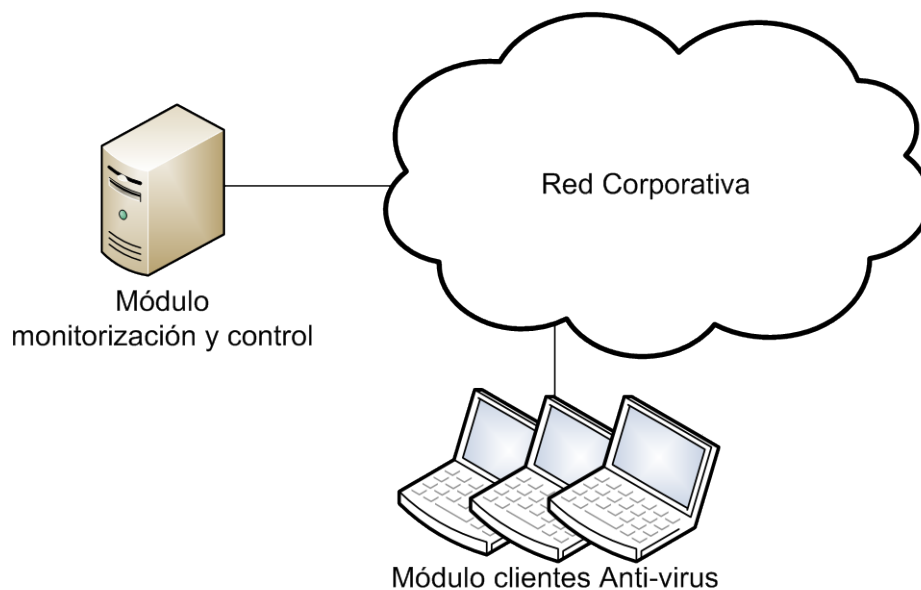


Figura 1 – Ejemplo de Caso de Uso: Gestión centralizada

2.2.2. CASO DE USO 2 - GESTIÓN INDIVIDUALIZADA

10. La gestión es autónoma en cada equipo, la monitorización y control de ejecución de la aplicación del Anti-virus forma parte de la propia aplicación.

2.3 ENTORNO DE USO

11. Por lo general, este tipo de dispositivos se encuentran en grandes o medianas empresas, así como en redes del sector público, como parte de una arquitectura de defensa en profundidad, en combinación con medidas complementarias en diferentes capas de protección.
12. Para la utilización en condiciones óptimas de seguridad de los sistemas para la prevención de fuga de datos, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:
 - **Plataforma segura:** El producto se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.
 - **Acceso:** El producto tiene acceso todos los datos del sistema necesarios para llevar a cabo todas sus funciones.
 - **Administración confiable:** El Administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la empresa/administración. Por ello se asume que dicha persona estará capacitada, formada y carecerá de cualquier intención dañina al administrar el producto.
 - **Actualizaciones periódicas:** El software del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

13. Este tipo de productos son herramientas que suelen presentarse en formato de software que se instala en un sistema de ficheros proporcionado por un sistema operativo. Se Ejecuta en una plataforma que puede ser el sistema operativo, un entorno de ejecución o una combinación de las anteriores.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

14. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TI (Tecnologías de la Información).
15. En el ámbito de CC se elaboran unos perfiles de seguridad que definen, para un dominio o categoría de productos, un conjunto de objetivos y requisitos de seguridad, tanto funcionales como de evaluación, independientes de la implantación.
16. Los productos dentro de esta familia deberán cumplir con los SFR (*Security Functional Requirements*) que se especifican en el siguiente perfil de protección certificado de acuerdo a la norma *Common Criteria*:

PERFIL DE PROTECCIÓN			
Perfil de protección	Versión	Fecha	Organismo responsable
<i>Protection Profile for Application Software.</i> ¹	1.2	25/04/2016	NIAP

Tabla 1. Perfil de protección

junto con los restantes requisitos fundamentales de seguridad recogidos en la sección 4.

17. El nivel de confianza EAL (*Evaluation Assurance Level*) con el que deben ser evaluados los requisitos exigidos para esta familia será:
- **El determinado por el perfil de protección** para aquellos SFR incluidos en el perfil exigido cuando los productos se encuentren certificados contra éste.
 - **EAL2 o superior** para los RFS adicionales que no encuentren incluidos dentro del perfil.
 - **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra el perfil.

¹https://www.commoncriteriaportal.org/files/ppfiles/pp_app_v1.2.pdf

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

18. Los recursos que es necesario proteger mediante el uso de esta familia de productos, incluyen:
- Comunicaciones con el producto.
 - Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos.
 - Datos de configuración del producto y de auditoría generados por éste.
 - Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

19. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente serían:
- **Ataque a la red.** Un atacante, que acceda al canal de comunicación, puede modificar las comunicaciones entre los distintos módulos del producto.
 - **Monitorización del tráfico.** Un atacante, desde dentro o desde fuera de la red, consigue acceder a información intercambiada entre los distintos módulos de la aplicación.
 - **Ataque local.** Un atacante puede actuar a través de software ejecutado en la misma plataforma de computación donde se ejecuta el producto. Los atacantes podrían modificar de forma maliciosa los ficheros o comunicaciones que utiliza el producto.
 - **Acceso físico.** Un atacante podría acceder a información sensible almacenada en el sistema.
 - **Auditoria.** Un usuario o proceso podría causar la pérdida o modificación de registros de auditoría del producto de forma maliciosa.
 - **Virus.** Un agente dañino podría intentar introducir un virus vía red o medios removibles que comprometa el sistema.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

20. A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a la inclusión en el CPSTIC en esta familia.

4.1 PERFIL DE PROTECCIÓN

21. **REQ. 1** El producto debe cumplir con los SFR (*Security Functional Requirements*) que se especifican el siguiente perfil de protección certificados de acuerdo a la norma *Common Criteria*:

PERFIL DE PROTECCIÓN			
Perfil de protección	Versión	Fecha	Organismo responsable
<i>Protection Profile for Application Software.</i> ²	1.2	25/04/2016	NIAP

Tabla 2. Perfil de protección

22. **REQ. 2** En caso de que el producto no esté certificado contra el perfil indicado, la declaración de seguridad deberá contener al menos los SFR de éste con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.2 REQUISITOS CRIPTOGRÁFICOS

23. **REQ. 3** Todos los algoritmos de cifrado simétrico, asimétrico, protocolos de acuerdo de clave y funciones resumen que utilice el producto deberán encontrarse dentro de los acreditados por el CCN para su uso en el ENS. El listado de dichos algoritmos se encuentra recogido en la CCN-STIC-807Criptología de empleo en el ENS (Categoría ALTA).

4.3 REGISTROS AUDITORIA

24. **REQ. 4** Se debe proporcionar un medio para almacenar los eventos relacionados con la seguridad, de forma que permita interpretarse por un usuario.
25. **REQ. 5** Los registros de auditoría contendrán al menos la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento.
26. **REQ. 6** Se registrarán en la auditoria los siguientes eventos:
- Acción tomada en respuesta a una detección de virus.
 - Detección de virus.

²https://www.commoncriteriaportal.org/files/ppfiles/pp_app_v1.2.pdf

- c. Iniciar o detener la auditoría de la aplicación.
 - d. Cambios en el grupo de usuario que tiene el rol de administrador.
 - e. Utilización por parte del usuario de los mecanismos de autenticación.
 - f. Cualquier utilización de los mecanismos de autenticación del producto.
 - g. Cambios de la configuración del producto.
27. **REQ. 7** Los registros de auditoría, no podrán modificarse por ningún usuario.
28. **REQ. 8** Sólo podrán leer los registros de auditoría los usuarios autorizados.
29. **REQ. 9** Los administradores serán los únicos usuarios que puedan borrar registros de auditoría.

4.4 IDENTIFICACIÓN Y AUTENTICACIÓN

30. **REQ. 10** El producto debe mantener una lista de atributos de seguridad perteneciente a cada usuario. Los atributos serán, al menos, los siguientes:
- a. Identificación única de usuario.
 - b. Contraseña / método de acceso.
 - c. Rol de usuario y su estado actual (habilitado o no).
31. **REQ. 11** El producto requerirá que cada usuario sea autenticado correctamente antes de permitir cualquier otra acción en el producto en nombre de ese usuario.

4.5 VIRUS

32. **REQ. 12** Una vez detectado un virus basado en memoria, se deberá bloquear la ejecución del virus.
33. **REQ. 13** Una vez detectado un virus basado en fichero, se deberán tomar las acciones previamente definidas por el administrador (limpiar fichero de virus, poner el fichero en cuarentena, borrar el fichero).
34. **REQ. 14** Una vez detectado un virus, el producto deberá mostrar una alerta en el equipo donde se ha detectado el virus. Se deberá mostrar el virus detectado y las acciones tomadas.
35. **REQ. 15** Una vez detectado un virus, el producto deberá alertar al administrador, indicando el nombre del equipo infectado, el virus detectado, las acciones tomadas por el producto.
36. **REQ. 16** El producto deberá escanear en tiempo real la memoria del sistema para detectar virus (firmas de virus conocidos) basados en memoria.
37. **REQ. 17** El producto deberá escanear a tiempo real, de forma programada y a demanda para detectar virus (firmas de virus conocidos) basados en ficheros.
38. **REQ. 18** El producto deberá escanear de forma programada a la hora y frecuencia definida por el administrador.

39. **REQ. 19** El producto permitirá escanear de forma manual, a petición de un usuario el equipo donde se ejecuta.

5. ABREVIATURAS

CC	<i>Common Criteria</i>
CCN	<i>Centro Criptológico Nacional</i>
CPSTIC	<i>Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones</i>
EAL	<i>Evaluation Assurance Level</i>
ENS	<i>Esquema Nacional de Seguridad</i>
EPP	<i>Endpoint Protection Platform</i>
NIAP	<i>National Information Assurance Partnership</i>
RFS	<i>Requisitos Fundamentales de Seguridad</i>
SFR	<i>Security Functional Requirements</i>