

Edita:



© Centro Criptológico Nacional, 2020
NIPO: 083-19-053-9

Fecha de Edición: Agosto 2020

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	3
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 DE DISPOSITIVOS MÓVILES.....	5
2.3 ENTORNO DE USO	6
2.4 DELIMITACIÓN DEL DISPOSITIVO EN ALCANCE	7
2.5 ALINEAMIENTO CON COMMON CRITERIA.....	7
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 REQUISITOS CRIPTOGRÁFICOS.....	9
4.2 PERFIL DE PROTECCIÓN SERVIDOR	9
4.3 PERFIL DE PROTECCIÓN AGENTE	9
4.4 CONFIGURACIÓN.....	10

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Herramientas de gestión de dispositivos (UEM¹)** 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.

NOTA: Esta familia recoge los requisitos de la familia “Herramientas de gestión de dispositivos Móviles (MDM)” y la sustituye en la Taxonomía de productos STIC.² En diferentes documentos pueden encontrarse referencias a este bloque funcional utilizando la denominación de MDM.

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 de gestión de dispositivos (UEM)** conforme a la taxonomía definida por el Centro

¹ UEM: *Unified Endpoint Management*

² La sucesiva aparición de nuevas funcionalidades y subcategorías dentro de las Herramientas de Gestión de Dispositivos Móviles (MDM), tales como MEM o MAM, junto con consideraciones desde el punto de vista legal ha dado lugar a la aparición de la familia de productos orientados a la Gestión de dispositivos. Estos productos ya no se orientan únicamente a la gestión de dispositivos móviles, si no que han evolucionado para poder gestionar casi cualquier dispositivo de usuario final (móviles, tabletas, ordenadores de sobremesa, ordenadores portátiles, dispositivos IoT,...)

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 cumplieren los RFS correspondientes.

2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS

2.1 FUNCIONALIDAD

6. Los productos asociados a esta familia permiten gestionar de forma eficiente la diversidad y el despliegue masivo, dinámico y a gran escala de dispositivos en una organización. Las herramientas de gestión de dispositivos móviles permiten aplicar políticas de seguridad y configuraciones a las diferentes familias de dispositivos de una organización de manera que dichos dispositivos puedan ser utilizados para procesar información o utilizar recursos de la organización conforme a los criterios establecidos por dicha organización.
7. La correcta aplicación de estas políticas debe ser la primera condición de una organización para permitir a cualquier dispositivo utilizar recursos propiedad o responsabilidad de la organización o manejar información y/o datos propiedad o responsabilidad de la organización.
8. Numerosos productos se han comercializado históricamente bajo otros acrónimos o incluyen funcionalidades complementarias a la de gestión del propio dispositivo, como puede ser MEM (Mobile Enterprise Management, Mobile Email Management), MCM (Mobile Content Management), MAM (Mobile Application Management), etc.
9. La evolución del mercado y diversas consideraciones legales han hecho que estas familias y subfamilias se agreguen actualmente bajo la denominación de Unified Endpoint Management. (Gestión de dispositivos de usuario final)
10. En la mayor parte de los casos, un mismo producto puede utilizarse para la gestión de diferentes dispositivos TIC (teléfonos móviles, ordenadores portátiles, ordenadores de sobremesa, Tabletas, etc.).

2.2 CASOS DE USO

2.2.1. CASO DE USO 1 – GESTIÓN DE DISPOSITIVOS MÓVILES

11. La herramienta de gestión de dispositivos (UEM) tendrá la funcionalidad de gestión de dispositivos. La arquitectura más habitual de este tipo de soluciones consta de una aplicación agente que se ejecuta sobre un dispositivo y un módulo servidor que se ejecuta en la infraestructura TIC de la organización. La aplicación agente establece una comunicación segura con el módulo servidor a través de una red no confiable.

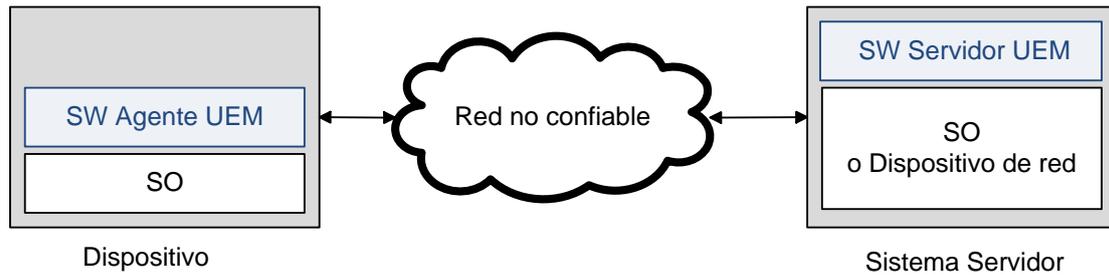


Figura 1 - Ejemplo de Caso de Uso 1: Gestión de dispositivos

12. El agente establece una comunicación segura con el servidor para consultar las políticas de seguridad de la organización y poder aplicarlas sobre el dispositivo.

2.3 ENTORNO DE USO

13. Estas herramientas pueden encontrarse tanto en empresas de diferente naturaleza, así como en redes de las Administraciones Públicas como parte de una arquitectura de defensa en profundidad que busca asegurar el entorno de comunicación para evitar escuchas o exfiltraciones de información, existiendo medidas complementarias en diferentes capas de protección.
14. Para la utilización en condiciones óptimas de seguridad de estos productos, es necesaria su integración en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:
 - **Entorno de ejecución seguro:** El producto, tanto el Agente como el Servidor, se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.
 - **Administración confiable:** El usuario 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 altamente capacitada y carecerá de cualquier intención maliciosa al administrar los dispositivos pasarelas. El producto no será capaz de defenderse contra un usuario administrador con malas intenciones.
 - **Actualizaciones periódicas:** El producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
 - **Protección de las comunicaciones:** Deberán habilitarse los mecanismos necesarios que permitan una comunicación segura entre los productos y las redes bajo control de la organización a las que estos se conecten (p.ej.: terminadores VPN/, puntos de acceso WLAN seguros, etc.).
 - **Protección de las credenciales:** Todas las credenciales, en especial la del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.

- **Política de seguridad de la información:** Una política de seguridad deberá recoger el conjunto de principios, organización y procedimientos definidos por la organización para hacer frente a sus necesidades de seguridad de la información, incluyendo el uso de las TIC.

2.4 DELIMITACIÓN DEL DISPOSITIVO EN ALCANCE

15. Este tipo de productos se presentan en formato de paquete software que se instala sobre una plataforma confiable.
16. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2.1, éstas quedan fuera del alcance analizado, debiendo ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 ALINEAMIENTO CON COMMON CRITERIA

17. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TIC (Tecnologías de la Información y de las Comunicaciones).
18. 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.
19. Los productos dentro de esta familia deberán estar certificados de acuerdo a la norma *Common Criteria*. Dicha certificación deberá evidenciar el problema de seguridad definido en el presente documento e incluir los requisitos fundamentales de seguridad recogidos en el apartado 4.
20. 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 los perfiles exigidos cuando los productos se encuentren certificados contra alguno de los perfiles anteriormente descritos.
 - **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra ningún perfil.
21. En caso de que alguno de los requisitos indicados en el apartado 4 no se encuentre recogido en la declaración de seguridad del producto, pero este sí implemente esa función de seguridad, se podrá llevar a cabo una **evaluación STIC complementaria**, cuyo objetivo será verificar el cumplimiento de esos requisitos.

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

22. Los recursos a proteger mediante el uso de estos productos, así como para su correcto funcionamiento, incluyen:
 - Información que intercambie el producto.
 - Información sensible que pueda almacenar el producto.
 - Datos de configuración del producto y de auditoría generados por éste.
 - Actualizaciones del producto susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

23. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente serían:
 - **Aplicaciones maliciosas o inseguras:** Las aplicaciones instaladas en el dispositivo pueden incluir código malicioso o explotable ya sea de manera intencionada o bien por un error en el desarrollo de la aplicación, pudiendo comprometer la confidencialidad, integridad y disponibilidad del dispositivo y su información.
 - **Envío de tráfico dañino:** Un atacante, enmascarado como un servidor de herramientas de gestión de dispositivos, puede intentar comprometer la integridad del dispositivo enviando comandos de configuración maliciosos.
 - **Acceso no autorizado:** un atacante puede interceptar las comunicaciones entre el servidor de la herramienta de gestión de dispositivos y el dispositivo para monitorizar, obtener acceso o modificar la información intercambiada.
 - **Acceso físico:** la pérdida, el robo o una mala custodia del dispositivo puede suponer el acceso a los datos de usuario o de la organización por parte de terceros.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

24. 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 REQUISITOS CRIPTOGRÁFICOS

25. **REQ. 1** 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-807 Criptología de empleo en el ENS (Categoría ALTA).

4.2 PERFIL DE PROTECCIÓN SERVIDOR

26. **REQ. 2** 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*:

PERFILES DE PROTECCIÓN			
Perfil de protección	Versión	Fecha	Organismo responsable
<i>Protection Profile for Mobile Device Management</i> ³	4.0	25/04/2019	NIAP
<i>Protection Profile for Mobile Device Management</i> ⁴	3.0	21/11/2016	NIAP

Tabla 1. Perfiles de protección MDM

27. **REQ. 3** En caso de que el producto no esté certificado contra el perfil indicado, la declaración de seguridad deberá contener al menos los SFR del perfil de protección *Protection Profile for Mobile Device Management* versión 4.0 con un nivel de confianza EAL (Evaluation Assurance Level) **EAL2 o superior**.

4.3 PERFIL DE PROTECCIÓN AGENTE

28. **REQ. 4** El producto deberá estar certificado o formar parte de una arquitectura con un producto certificado contra el siguiente perfil de protección:

³ https://www.niap-ccevs.org/MMO/pp/pp_mdm_v4.0.pdf

⁴ https://www.niap-ccevs.org/MMO/pp/pp_mdm_v3.0.pdf

PERFILES DE PROTECCIÓN			
Perfil de protección	Versión	Fecha	Organismo responsable
<i>Extended Package for Mobile Device Management Agents</i> ⁵	3.0	21/11/2016	NIAP

Tabla 2. Perfiles de protección agentes MDM

4.4 CONFIGURACIÓN

29. **REQ. 5** El producto debe poder desplegarse en una red conforme a las directrices establecidas en el documento “CCN-STIC 496 *Sistemas de Comunicaciones Móviles*” y definir y aplicar políticas de seguridad conforme a las directrices incluidas en el documento “CCN-STIC-827 *Gestión y uso de dispositivos móviles*”.

⁵ https://www.commoncriteriaportal.org/files/ppfiles/ep_mdm_agent_v3.0.pdf