centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC-
Anexo F.1: Dispositivos móviles

Febrero 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2019.02.27 09:41:35 +01'00'

NIPO: 083-19-053-9.

Fecha de Edición: febrero de 2019

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

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Dispositivos Móviles** 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, 3imo 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 **Dispositivos Móviles** 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. Los productos asociados a esta familia están orientados a la protección de equipos y servicios que proporcionan un medio de conexión sin cables (GSM[1], GPRS[2], UMTS[3], LTE[4], NFC[5], wifi[6], Bluetooth[7], etc.) junto con software específico para funciones tales como: mensajería segura, correo electrónico, acceso web, conexión VPN[8], VoIP[9] (Voz sobre IP), o conectividad contra una red corporativa protegida que ofrece servicios o datos específicos.

7. En este contexto proporcionan las siguientes funciones básicas de seguridad:

   - Políticas y mecanismos de seguridad para el control de acceso, integridad y confidencialidad en relación a los usuarios, la información y las aplicaciones del dispositivo.
   - Disponibilidad de mecanismos criptográficos para comunicaciones y transmisiones seguras.
   - Protección de información almacenada en el dispositivo.
   - Almacén de claves para su uso seguro en las aplicaciones instaladas en el dispositivo.

2.2 CASOS DE USO

8. En el caso de los productos de esta familia se contemplan tres casos de uso, en función de que la gestión de la red requiera o no de agentes desplegados en los sistemas involucrados. Las políticas de seguridad con las que se configura el producto pueden variar en cada caso, incluyendo más o menos restricciones.

2.2.1. CASO DE USO 1 – DISPOSITIVO PROPIEDAD DE LA ORGANIZACIÓN PARA USO CORPORATIVO GENERAL Y PARA USO PERSONAL LIMITADO.

9. El dispositivo es propiedad de la organización que lo cede a un empleado. En este caso la organización ejerce un cierto control sobre la configuración y el software del dispositivo. La organización lo cede al empleado para que haga uso de servicios como VPN o el correo electrónico corporativo manteniendo el control y la seguridad de los datos y las redes corporativas. El empleado puede

[1] *Global System for Mobile communications.*Sistema global para las comunicaciones móviles
[2] *General Packet Radio Service*. Servicio general de paquetes vía radio
[3] *Universal Mobile Telecommunications System.* Sistema universal de telecomunicaciones móviles
[4] *Long Term Evolution*. Evolución de largo plazo
[5] *Near Field communication*. Comunicación de campo cercano
[6] *Wireless Fidelity*
[7] Protocolo de comunicaciones para redes inalámbricas de área personal
[8] *Virtual Private Network*
[9] Voz sobre el protocolo de Internet

utilizar el dispositivo para acceder a dichos servicios y además determinados usos personales, cómo el acceso a Internet, a través de la red corporativa.

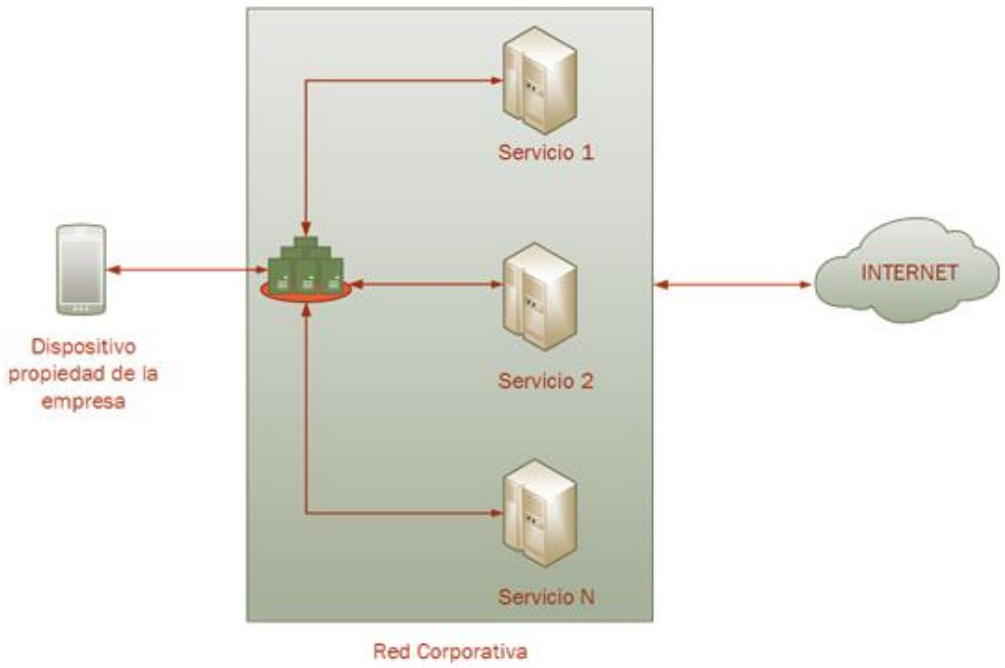

Figura 1. Ejemplo de Caso de Uso 1: Dispositivo propiedad de la empresa para uso corporativo general y para uso personal limitado.

2.2.2. CASO DE USO 2 – DISPOSITIVO PROPIEDAD DE LA ORGANIZACIÓN PARA USO DE ALTA SEGURIDAD

10. El dispositivo es propiedad de la organización que lo cede a un empleado. En este caso la organización se autoexige un alto control sobre la configuración y el software del dispositivo está limitado para su uso para manejar o utilizar servicios que tratan con información sensible. El dispositivo sólo podrá conectarse a la red corporativa, en caso de que las políticas de la organización permitan acceso a servicios corporativos a Internet, el dispositivo accederá a través de la red corporativa.

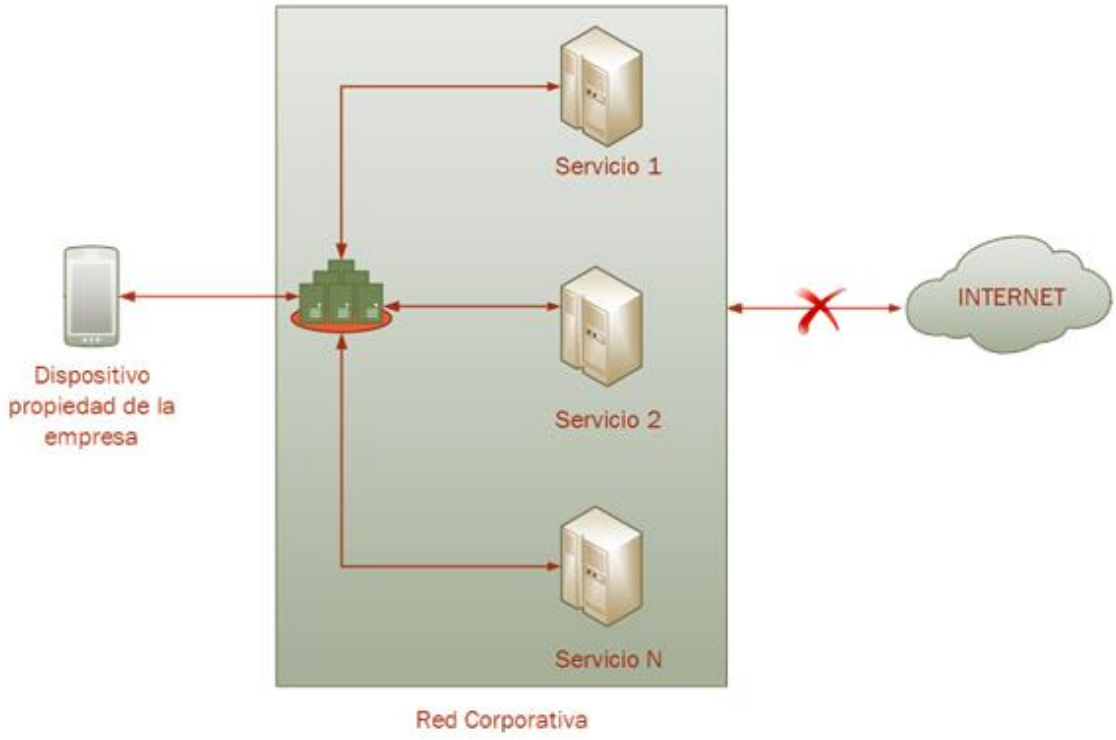

Figura 2 Ejemplo de Caso de Uso 2: Dispositivo propiedad de la empresa para uso de alta seguridad.

2.2.3. CASO DE USO 3 – DISPOSITIVO PROPIEDAD DEL EMPLEADO PARA USO PERSONAL Y CORPORATIVO

11. El dispositivo es propiedad de un empleado de la organización. En este caso la organización provee al dispositivo con los recursos necesarios para lograr el acceso a la red corporativa y los servicios que ofrece. Esta práctica se conoce bajo su denominación en inglés *Bring Your Own Device* (BYOD). La organización no tendrá control sobre la configuración y por tanto deberá implementar controles de seguridad para mitigar los posibles incidentes que puedan producirse. Estos controles pueden incluir una aplicación específica, mecanismos físicos a incluir en el dispositivo, etc. La organización deberá tener en cuenta la normativa y la seguridad jurídica que implica la utilización de un dispositivo propiedad del empleado para su uso corporativo.

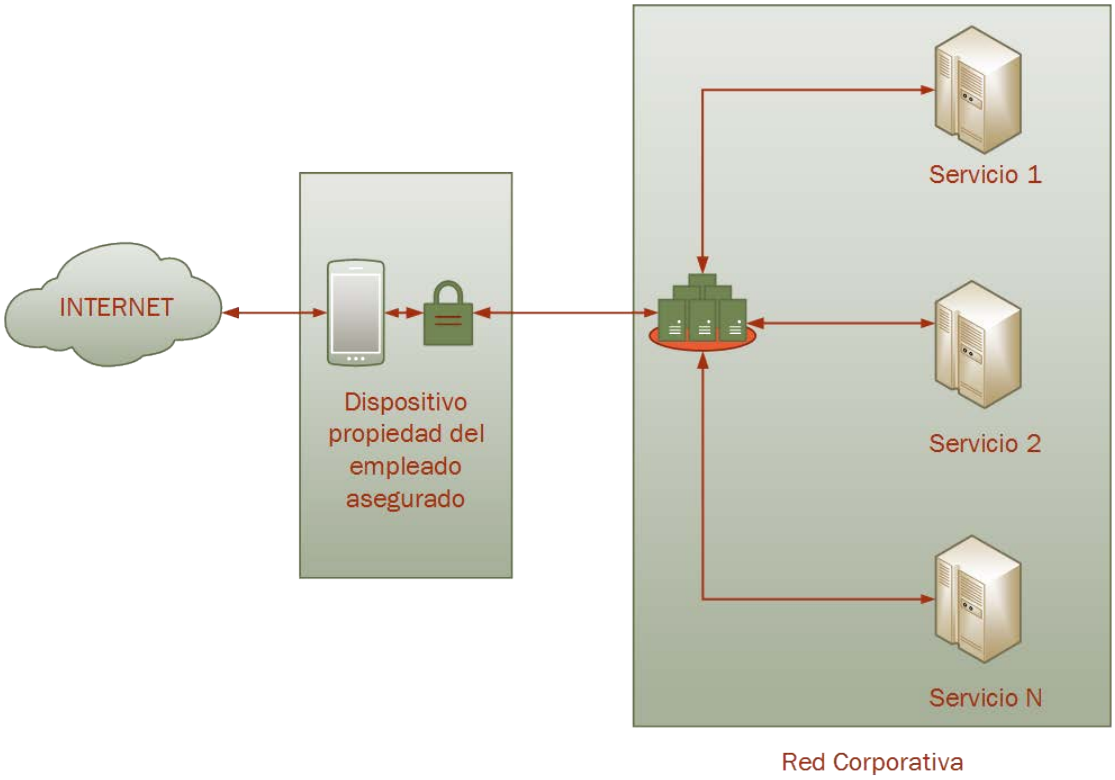

Figura 3 Ejemplo de Caso de Uso 3: Dispositivo propiedad del empleado para uso personal y corporativo (BYOD).

2.3 ENTORNO DE USO

12. Por lo general, este tipo de dispositivos se encuentran en cualquier tipo de ámbito, debido a su actual trascendencia para la sociedad de la información, tanto en el caso de usuarios privados, como de empresas y usuarios del sector público. En particular es común su uso por parte de empleados que por necesidades de negocio están continuamente desplazándose y por ello necesitan un medio de acceso a la red corporativa transportable y también para el manejo de infraestructuras o servicios que necesitan utilizar este tipo de dispositivos para su funcionamiento.

13. Para la utilización en condiciones óptimas de seguridad, es necesaria su integración en un entorno operacional que cumple las siguientes condiciones mínimas de protección:

    - **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 producto será puesto al día conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.

- **Protección de las credenciales:** Todas las credenciales, en especial las de administración, deberán estar correctamente protegidas por parte de la organización y los usuarios que utilicen el producto.
- **Protección de las comunicaciones.** Deberán habilitarse los mecanismos necesarios que permitan una comunicación segura, así como las redes a las que estos se conecten bajo el control de la organización.
- **Política de seguridad de la información.** La política de seguridad deberá recoger el conjunto de principios, procedimientos y marco organizativo impuestos por una entidad para hacer frente a sus necesidades de seguridad de la información, incluyendo el uso de las TIC.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

14. Este tipo de productos son dispositivos que cuentan con una plataforma **Hardware**, con un Firmware y un Software básico incorporado (incluyendo su correspondiente **Sistema Operativo**). Sobre éstos, se diseñan e instalan **aplicaciones o utilidades Software** que añaden servicios como los citados en la sección 2.1.
15. 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 CRITERIOS COMUNES (COMMON CRITERIA)

16. 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).
17. 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.
18. Los productos dentro de esta familia deberán cumplir con los requisitos Fundamentales de Seguridad reflejados en el apartado 4 y con los SFR (*Security Functional Requirements*) que se especifican en alguno de los siguientes perfiles de protección certificados de acuerdo a la norma *Common Criteria:*

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Mobile Device Fundamentals[10]	3.0	10/06/2016	NIAP
Protection Profile for Mobile Device Fundamentals[11]	3.1	16/06/2017	NIAP
Protection Profile for Trusted platform for secure communications. EAL2+[12]	1.0	29/09/2016	CCN

Tabla 1. Perfiles de protección

19. En caso de que el producto no esté certificado contra ningún perfil de los anteriores, la declaración de seguridad deberá contener al menos los SFR de uno de ellos con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

[10] https://www.commoncriteriaportal.org/files/ppfiles/PP_MD_V3.0.pdf
[11] https://www.commoncriteriaportal.org/files/ppfiles/PP_MD_V3.1.pdf
[12] https://www.commoncriteriaportal.org/files/ppfiles/ccn-pp-tp_eal2_v1.0.pdf

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

20. Los recursos a proteger mediante el uso de estos productos, así como para su correcto funcionamiento, incluyen:

    - Información que intercambie el producto entre sus interfaces de red y la red corporativa, en ambos sentidos.
    - Información sensible que pueda almacenar el dispositivo en su almacenamiento interno (p.e.: memoria interna volátil y no volátil) o en dispositivos extraíbles (p.ej.: memorias microSD[13]).
    - Información sensible que pueda ser captada a través de periféricos y sensores con que se encuentre equipado el dispositivo (p.ej.: cámaras o micrófonos integrados, GPS, etc.)
    - 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

21. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente serían:

    - **Divulgación de la información no autorizada.** Un atacante consigue recopilar información no autorizada del dispositivo (p.ej. información corporativa sensible, conversaciones, datos de posicionamiento, etc.).
    - **Acceso no autorizado**: Un atacante ya sea desde dentro de la red o desde fuera consigue acceder a información, intercambiada a través del dispositivo, así como generada o almacenada en él, para la que no estaba autorizado (p.ej.: información almacenada en memoria o imágenes captadas por una cámara integrada en el dispositivo) o utilizar el dispositivo como mecanismo de acceso a la red corporativa. Estas amenazas incluyen el intento de acceso físico al dispositivo a través de puertos de conexión hardware externos, mediante la imitación de mecanismos de autenticación del usuario, o bien a través de un acceso directo y posiblemente destructivo a sus medios de almacenamiento.
    - **Envío de tráfico dañino**: Un atacante consigue enviar información de manera malintencionada, con el fin de poner en riesgo la seguridad de éste o de aquellos otros recursos a los que se conecta (p.ej. páginas web con código dañino incorporado o ficheros adjuntos en correos electrónicos).
    - **Cifrado débil.** Utilización en el dispositivo de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente, mediante ataques de fuerza bruta.

[13] Tarjeta de memoria Secure Digital micro (15x11x1)

- **Uso de canales de comunicación inseguros.** Permiten a un atacante comprometer la integridad y la confidencialidad de las comunicaciones del producto.
- **Compromiso de la funcionalidad del dispositivo.** Un atacante o un fallo en el dispositivo compromete la funcionalidad de seguridad, permitiendo modificarla o desactivarla de manera no conforme a las políticas de seguridad (p.ej., instalación de actualizaciones maliciosas o administración no autorizada del dispositivo).
- **Aplicaciones maliciosas o inseguras:** Las aplicaciones instaladas en el dispositivo móvil 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.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

22. 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

23. **REQ. 1** Los productos deberán estar certificados con uno de los siguientes perfiles de protección certificados de acuerdo a la norma *Common Criteria:*

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Mobile Device Fundamentals[14]	3.0	10/06/2016	NIAP
Protection Profile for Mobile Device Fundamentals[15]	3.1	16/06/2017	NIAP
Protection Profile for Trusted platform for secure communications. EAL2+[16]	1.0	29/09/2016	CCN

Tabla 2. Perfiles de protección

24. **REQ. 2** En caso de que el producto no esté certificado contra ningún perfil de los anteriores, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) de uno de ellos con un nivel de confianza **EAL2 o superior**.

4.2 CONFIGURACIÓN

25. **REQ. 3** Los productos deberán poder configurarse conforme a las directrices incluidas en el documento CCN-STIC 827.Gestión y uso de dispositivos móviles[17].

[14] https://www.commoncriteriaportal.org/files/ppfiles/PP_MD_V3.0.pdf
[15] https://www.commoncriteriaportal.org/files/ppfiles/PP_MD_V3.1.pdf
[16] https://www.commoncriteriaportal.org/files/ppfiles/ccn-pp-tp_eal2_v1.0.pdf
[17] https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/544-ccn-stic-827-gestion-y-uso-de-dispositivos-moviles/file.html

5. ABREVIATURAS

BYOD	Bring your own device
CC	Common Criteria
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
EAL	Evaluation Assurance Level
ENS	Esquema Nacional de Seguridad
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
IP	Internet Protocol
LTE	Long Term Evolution
NFC	Near Field Communication
NIAP	National Information Assurance Partnership
RFS	Requisitos Fundamentales de Seguridad
SD	Secure Digital
SFR	Security Functional Requirements
UTMS	Universal Mobile Telecommunications System
VoIP	Voz sobre IP
VPN	Virtual Private Network
WIFI	Wireless Fidelity