GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC - Anexo F.2: Sistemas operativos

Noviembre 2017

Edita:

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
2017.11.27 11:28:54 +01'00'

NIPO: 785-17-037-2.

Fecha de Edición: noviembre 2017
ISDEFE ha participado en el desarrollo del presente documento.

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Sistemas Operativos** 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 **Sistemas Operativos** 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 utilizan software que administra recursos de hardware y software, y proporciona servicios comunes para aplicaciones. El hardware que gestionan puede ser físico o virtual. Estos productos están formados por el núcleo del sistema operativo y sus controladores, bibliotecas de software compartidas y alguna aplicación software incluida con el sistema operativo. Estas aplicaciones son aquellas que proporcionan servicios de seguridad esenciales, muchas de las cuales necesitan ejecutarse con privilegios elevados. Algunas de estas aplicaciones requerirán el cumplimiento de otros RFS adicionales (p.ej.: aplicaciones VPN).

7. Si bien estos productos no tienen como objeto proporcionar seguridad a las TIC, sí que llevan intrínsecamente asociados mecanismos de seguridad que los protejan frente a las múltiples amenazas a que se exponen, tanto por la amplia difusión de su uso, como por el control que ofrecen sobre los procesos básicos que dan soporte a los servicios TIC y su elevada superficie de exposición como principal interfaz con los usuarios. En este contexto las funciones básicas de seguridad que proporciona esta familia de productos son las siguientes:

    - **Protección de la información, recursos y funciones básicas del sistema.** Los sistemas operativos proporcionan mecanismos para proteger el acceso a los recursos que manejan (p.ej. procesadores, memoria, dispositivos I/O, etc.) y las funciones básicas que pone a disposición de los servicios a los que da soporte, velando también por la integridad de los datos que procesan y guardan en los medios de almacenamiento.
    - **Administración confiable.** Los productos de esta categoría facilitan la administración de los mismos mediante interfaces seguras y adecuadas al nivel de protección requerido. Esto incluye mecanismos y métodos seguros para el despliegue de actualizaciones y para el control de ejecución de aplicaciones.
    - **Protección de las comunicaciones.** Estos productos ofrecen medidas para establecer canales de comunicación seguros ya sea entre conexiones con otros productos y/o dispositivos, así como a nivel local utilizando mecanismos para proteger la información en tránsito.
    - **Gestión de registros.** Los sistemas operativos proporcionan mecanismos para el registro de los eventos en el sistema, que faciliten información útil para el mantenimiento y aseguramiento de la disponibilidad, así como para la auditoría de seguridad frente a incidentes.

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 tres casos de uso para esta familia de productos tal y como se definen a continuación.

2.2.1. CASO DE USO 1 – SISTEMA OPERATIVO PARA USUARIO FINAL

9. El producto está destinado a usuarios finales y, por tanto, consumidores de servicios más que generadores de los mismos. Ocasionalmente pueden cubrir tareas de servidores de administración también. Estos sistemas operativos estarán desplegados en dispositivos tales como ordenadores de sobremesa, pero también en equipos portátiles o dispositivos convertibles.
10. También es posible que cubran dispositivos móviles o tabletas (*tablets*) pero en ese caso deberán ser evaluados frente al RFS de la familia de Dispositivos móviles.
11. Dentro de la arquitectura de red de la organización, estos productos pueden encontrarse en cualquier punto donde haya un usuario final del servicio.

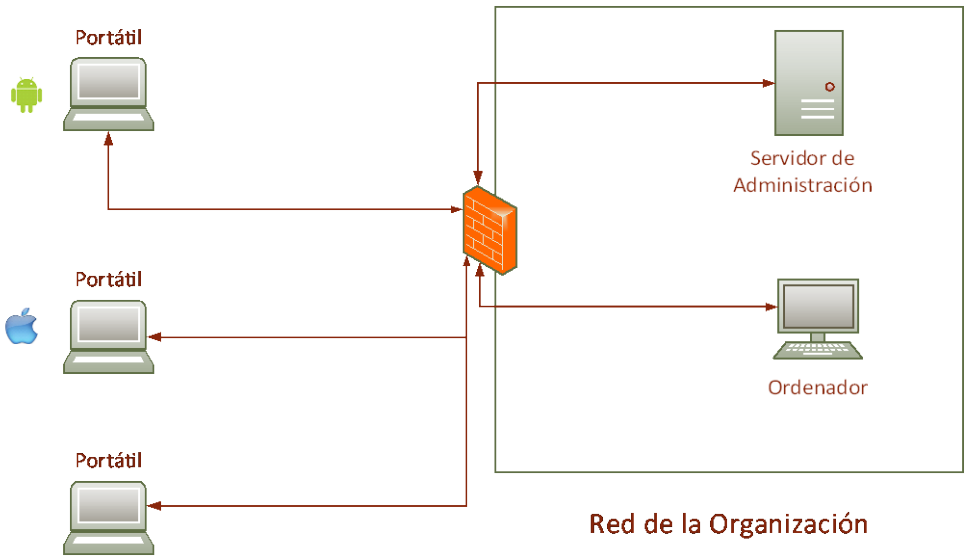

Figura 1. Ejemplo de Caso de Uso 1: Sistema Operativo para usuario final

2.2.2. CASO DE USO 2 – SISTEMA OPERATIVO PARA EQUIPO SERVIDOR

12. En este caso de uso, los sistemas operativos están destinados a funcionar en máquinas de tipo servidor ya sean físicas o virtuales, para ofrecer cualquier tipo de servicio a otros sistemas o usuarios finales (p.ej.: servidor de ficheros, correo, web, etc.).
13. Estos productos se despliegan dentro de la red de una organización proporcionando servicios al resto de componentes y usuarios de la organización o al exterior a través de interfaces con otras redes como Internet.

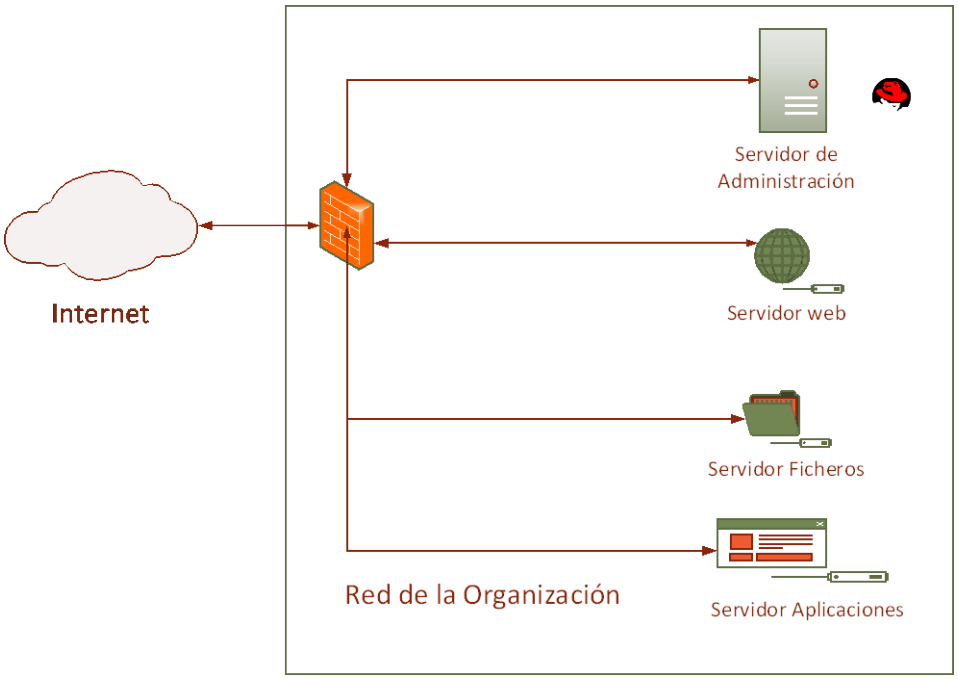

Figura 2. Ejemplo de Caso de Uso 2: Sistema Operativo para equipo servidor

2.2.3. CASO DE USO 3 – SISTEMA OPERATIVO EN LA NUBE (*CLOUD*)

14. El producto proporciona una plataforma para proveer servicios en la nube que se ejecutan en hardware ya sea físico o virtual. Un sistema operativo suele formar parte de ofertas identificadas como infraestructura como servicio (IaaS[1]), software como servicio (SaaS[2]) y plataforma como servicio (PaaS[3]).
15. Dentro de la arquitectura de red de la organización, estos productos se encuentran dentro de la red de la organización en un sistema propio específico para otorgar servicios desde la nube (*Cloud System*) proporcionando sistemas operativos como parte de los servicios SaaS, IaaS o PaaS.

[1] *Infrastructure as a Service*
[2] *Software as a Service*
[3] *Platform as a Service*

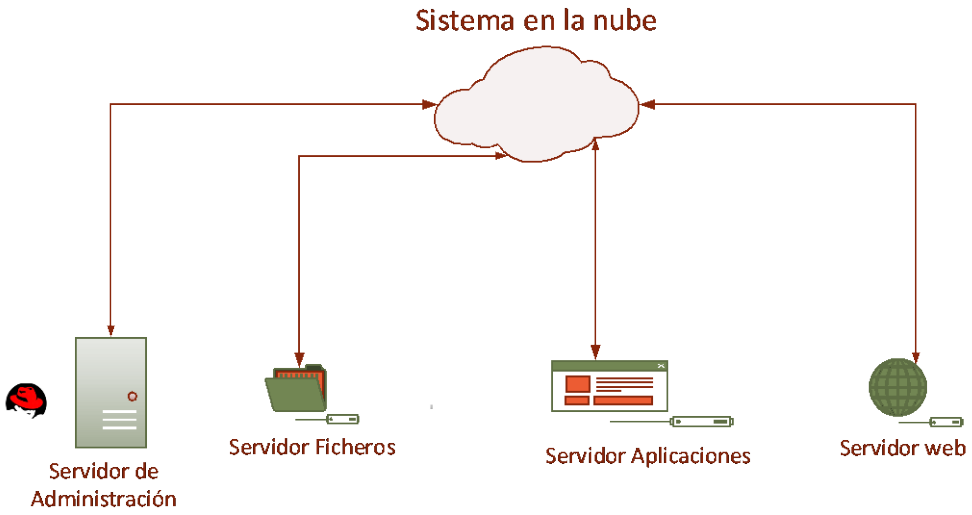

Figura 3. Ejemplo de Caso de Uso 3: Sistema Operativo en la nube (*cloud*)

2.3 ENTORNO DE USO

16. Estos productos se encuentran en una gran mayoría de dispositivos electrónicos, y en particular su uso es intensivo en las redes TIC de hogares o empresas, así como del sector público.

17. Para la utilización en condiciones óptimas de seguridad, es necesaria su integración en un entorno operacional que cumpla 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 maliciosa 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 la del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.
    - **Protección de la información**. El entorno debe proteger los datos del producto y de los dispositivos y servicios que se encuentran desplegados/instalados en él y garantizar que estos estén configurados correctamente y sean seguros.
    - **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[4]/SSH[5], puntos de acceso WLAN[6] seguros, etc.).

- **Política de seguridad de la Información.** La política de seguridad deberá recoger el conjunto de principios, organización y procedimientos impuestos por una 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

18. Este tipo de productos se presentan en formato de paquete **Software**, generalmente desplegado sobre un equipamiento Hardware dedicado, para administrar sus recursos, así como el software a través del que proporcionar servicios y/o aplicaciones necesarias para la organización, usuario, etc. También es común su despliegue en entornos virtuales, permitiendo la ejecución concurrente e independiente de múltiples sistemas operativos sobre unos recursos hardware compartidos.
19. En el caso particular de sistemas operativos para dispositivos móviles, quedarían fuera del alcance de este RFS cuando sean específicamente evaluados contra el RFS de Dispositivos Móviles, no requiriéndose el cumplimiento de ambos.
20. 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 (p.ej. almacenamiento cifrado de datos, sistemas de virtualización, etc.).

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

21. 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).
22. 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.
23. 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 especifica en el siguiente perfil de protección certificado de acuerdo a la norma *Common Criteria:*

[4] *Virtual Private Network*
[5] *Secure SHell,. intérprete de órdenes seguro*
[6] *Wireless local area network*

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for General Purpose Operating Systems.[7]	4.1	09/03/2016	NIAP

Tabla 1. Perfil de protección

24. En caso de que el producto no esté certificado bajo 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**.

[7] https://www.commoncriteriaportal.org/files/ppfiles/pp_os_v4.1.pdf

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS A PROTEGER

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

    - Credenciales de los usuarios y los servicios a los que es posible acceder desde la red corporativa.
    - Información sensible que pueda almacenar el producto en su configuración o en el dispositivo hardware donde haya sido desplegado.
    - Información sensible que pueda ser captada a través de periféricos y sensores con que se encuentre equipado el dispositivo.
    - 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

26. Las principales amenazas deliberadas a las que el uso de esta familia de productos pretende hacer frente, atendiendo a los casos de uso expuestos conforme a la sección 2.2, serían:

    - **Divulgación de información no autorizada:** Un atacante consigue recopilar información no autorizada del producto (p.ej. servicios de la organización, credenciales, etc.).
    - **Escucha de red:** Un atacante consigue infiltrarse hasta un punto de conexión de la infraestructura de red. El atacante puede supervisar y obtener acceso a la comunicación y/o los datos intercambiados (p.ej. credenciales de usuarios) entre el producto y otros puntos finales de la red corporativa que no son los escogidos de forma deliberada para el estudio de los ataques.
    - **Acceso no autorizado**: Un atacante consigue acceder a información, intercambiada a través del producto, así como generada o almacenada en él, para la que no estaba autorizado (p.ej.: información almacenada memoria).
    - **Suplantación de la identidad de usuarios registrados.** El atacante suplanta la identidad de usuarios legítimos mediante la apropiación de credenciales o medios de entrada ajenos, pudiendo obtener acceso al producto o a los servicios que estaban reservados a dichos usuarios. Este tipo de ataques activos pueden utilizar técnicas de ataques tales como explotación de contraseñas, secuestro de sesión, ataques *hombre en el medio,* robo de dispositivos, etc.

- **Cifrado débil**: Utilización en el producto de algoritmos criptográficos débiles que permitan a un atacante comprometerlo o averiguar su funcionamiento para lograr descifrar la información tratada en él.
- **Uso de canales de comunicación inseguros**: Mala implementación de protocolos estándar o utilización de protocolos no estandarizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones del producto.
- **Compromiso de la funcionalidad del producto**: Un atacante o un fallo en la herramienta compromete la funcionalidad de seguridad, permitiendo modificarla de manera no conforme a las políticas de seguridad (p.ej.: instalación de actualizaciones maliciosas o administración no autorizada).

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

27. 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

28. **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**
Protection Profile for General Purpose Operating Systems.[8]	4.1	09/03/2016	NIAP

Tabla 2. Perfil de protección

29. **REQ. 2** El producto deberá cumplir con los requisitos funcionales del perfil de protección de la tabla 2 considerados como opcionales, recogidos en el apéndice A del documento (*FCS_TLSC_EXT.4 y FTA_TAB.1*).

30. **REQ. 3** En caso de que el producto no esté certificado bajo el perfil indicado, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) de éste con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.2 REQUISITOS CRIPTOGRÁFICOS

31. **REQ. 4** 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).

[8] https://www.commoncriteriaportal.org/files/ppfiles/pp_os_v4.1.pdf

5. ABREVIATURAS

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*

IaaS *Infrastructure as a Service*

NIAP *National Information Assurance Partnership*

PaaS *Platform as a Service*

RFS *Requisitos Fundamentales de Seguridad*

SaaS *Software as a Service*

SFR *Security Functional Requirements*

SS *Secure SHell*

VPN *Virtual Private Network*

WLAN *Wireless local area network*