centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC-
Anexo F.7: Virtualización

Julio 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN
centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.07.19 10:04:30 +02'00'

NIPO: 083-19-053-9.

Fecha de Edición: julio 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 **Virtualización** 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 los 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 **Virtualización** 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 la familia de Virtualización están orientados fundamentalmente a aprovechar una misma infraestructura hardware bajo un sistema operativo (SO), denominado SO anfitrión, que se compartirá con múltiples entornos aislados cada uno con su propio SO, llamado SO invitado, posibilitando la mejora en la eficiencia y flexibilidad de los recursos TIC. El **hipervisor, o Monitor de Máquinas Virtuales (VMM)**, es el componente del producto que permite al equipo físico soportar los distintos entornos virtuales con sus configuraciones. Cada entorno virtual se encapsula en **una máquina virtual (VM)** que tiene asignados unos recursos virtuales, como memoria, procesador, SO invitado y aplicaciones.

7. El principal objetivo de la virtualización es incrementar la flexibilidad y la eficiencia en las TIC mediante la compartición de recursos entre distintos entornos. Por ello, en líneas generales, los productos se verán afectados por casi las mismas amenazas que los sistemas sin virtualizar más aquellas derivadas de dicha compartición.

8. Además, en algunos casos la virtualización podría emplearse como elemento de seguridad, por diversos motivos:

    a) Puede reducir la superficie de ataque considerablemente.

    b) Permite encapsular SO heredados que no puedan alcanzar una protección adecuada por ellos mismos.

    c) Puede utilizarse para proporcionar un entorno base seguro de trabajo a los usuarios, agilizando la gestión de incidentes en el aislamiento de un entorno infectado y restaurándolo con otro limpio.

9. En este contexto, las funciones básicas de seguridad que proporcionan esta familia de productos son las siguientes:

    a) **Protección de la información, recursos y funciones básicas del sistema**. Desde la virtualización se proporcionan mecanismos para proteger el acceso a los recursos que maneja (p.ej. procesadores, memoria, SO, dispositivos I/O, etc.) y al hipervisor, velando también por la integridad de los datos que se procesan y se guardan en los medios virtuales de almacenamiento.

    b) **Administración confiable**. Los productos de esta categoría facilitan su administración 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.

c) **Protección de las comunicaciones.** Estos productos ofrecen medidas para establecer canales de comunicación seguros entre el hipervisor y los entornos virtuales.

d) **Gestión de registros de auditoría.** La virtualización proporciona 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

10. Los productos de esta familia responden al caso de uso: **Herramientas de Virtualización de Servidor.**

11. La virtualización de servidor es la arquitectura más tradicional de virtualización. Mediante tecnología software permite la ejecución de varios sistemas operativos diferentes entre sí, como invitados dentro de un único servidor físico (*host*). Esto son las llamadas **Máquinas Virtuales (VM)** que se ejecutan en una imitación virtual del hardware del servidor.

12. Las tecnologías de virtualización de servidor normalmente se basan en el uso del **Hipervisor o Monitor de Máquina Virtual (VMM)**, que es el software que presenta a los sistemas operativos virtualizados (SO invitados) una plataforma operativa virtual (hardware virtual), a la vez que ocultan a dicho sistema operativo virtualizado las características físicas reales de la plataforma en la que operan.

13. La ejecución del sistema operativo invitado bajo el control del hipervisor proporciona una *sandbox*, lo que permite reducir la superficie de ataque frente a la que proporciona el sistema operativo del host, por lo que disminuye la posibilidad de expansión de un ataque exitoso fuera del SO invitado.

14. En caso de infección de un SO invitado es posible, además, guardar una copia para su posterior análisis, y recuperar un estado no infectado mediante la utilización de imágenes almacenadas previamente, que proporcionan una línea base de seguridad en la configuración.

15. La virtualización de servidor se emplea con mucha frecuencia para asegurar sistemas operativos obsoletos (*legacy*). Al ejecutarlos como un SO invitado, el hipervisor puede monitorizarlos aplicando controles de seguridad que el SO obsoleto por sí mismo no podría aplicar.

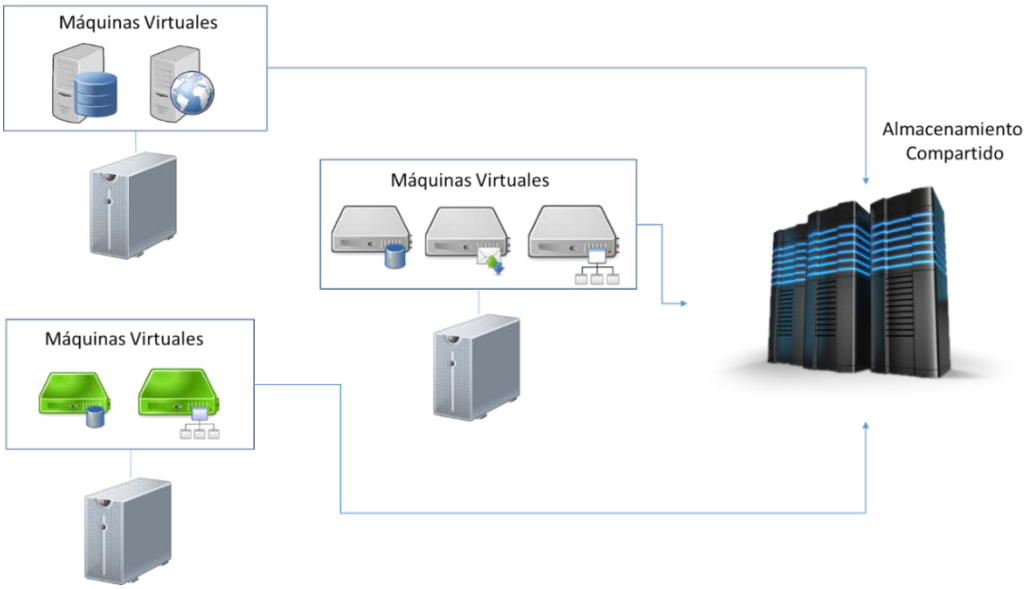

Figura 1. Ejemplo de Caso de Uso: Virtualización de Servidores.

2.3 ENTORNO DE USO

16. Gracias a la optimización de recursos que supone el uso de este tipo de productos, se encuentran cada vez más extendidos en grandes o medianas empresas, así como en las Administraciones Públicas. A su expansión contribuye también forma indirecta, el uso cada vez más extendido de las infraestructuras *cloud* (en la nube), que hacen uso de estas tecnologías de virtualización.

17. Para la utilización de estos productos en condiciones óptimas de seguridad, es necesaria su integración en un entorno operacional que cumpla las siguientes condiciones mínimas de protección:

    a) **Protección física:** las plataformas hardware sobre las que se emplee la herramienta de virtualización, deberán instalarse en áreas donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.

    b) **Integridad de la plataforma:** la plataforma no debe haber sido comprometida con anterioridad a la instalación del sistema de virtualización.

    c) **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 altamente capacitada y carecerá de cualquier intención maliciosa al administrar el hipervisor. El producto no será capaz de defenderse contra un usuario administrador con malas intenciones.

    d) **Usuarios confiables:** los usuarios no serán negligentes u hostiles de forma intencionada, y harán uso del sistema cumpliendo con la política de seguridad y con las guías de la organización.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

18. Este tipo de productos se presentan en formato de paquete Software, que se instalará sobre los equipos Hardware para crear las distintas máquinas virtuales atendiendo a los casos de uso anteriormente expuestos.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

19. 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).

20. En el ámbito de CC se elaboran unos perfiles de seguridad (*Protection Profiles*) 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.

21. Los productos dentro de esta familia deberán cumplir con los RFS reflejados en el apartado 4 y con los SFR (*Security Functional Requirements*) que se especifican en 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 Virtualization[1]	1.0	17/11/2016	NIAP
Protection Profile for Server Virtualization[2]	1.1	14/09/2015	NIAP

Tabla 1. Perfiles de protección

22. En caso de que el producto no esté certificado contra el perfil anterior, la declaración de seguridad deberá contener, al menos, los SFR (*Security Functional Requirements*) indicados en la Tabla 2 del apartado 4, con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2** o superior.

[1] https://www.niap-ccevs.org/MMO/PP/pp_base_virtualization_v1.0.pdf
[2] https://www.niap-ccevs.org/MMO/PP/pp_sv_v1.1.pdf

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

23. Los recursos que deben proteger estos productos incluyen:

- **Datos de usuario de cada VM**, de forma que no puedan filtrarse o ser accedidos por otras VMs a través de ningún recurso de la plataforma ni mecanismos de intercambio de datos no autorizados.
- **Software y aplicaciones que se ejecutan en una VM**, y que no deben ser interferidas por otras VMs.
- **Recursos físicos (CPU, memoria, I/O, almacenamiento, etc.) de la plataforma**, de forma que ninguna VM pueda afectar negativamente o acceder de forma no autorizada a recursos asignados a otra VM.
- **Integridad de la Plataforma**, de forma que ningún usuario o aplicación de alguna VM pueda socavar la integridad de la plataforma.
- **Funcionalidad y datos de configuración del producto y de auditoría** generados por este.

3.2 AMENAZAS

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

a) **Divulgación de información:** que los datos se filtren entre VMs a pesar de estar prohibido por la política. Esto permitiría que un atacante desde una VM pudiese obtener datos de otra VM causando con ello, que información sensible sea divulgada a entidades no autorizadas.

b) **Actualizaciones no autorizadas:** que un atacante pueda hacer pasar por auténtica su propia actualización, tomar control y comprometer el sistema de virtualización.

c) **Modificaciones no autorizadas:** que un malware que se esté ejecutando en la plataforma o en alguna VM pueda modificar los componentes del sistema de virtualización de forma indetectable.

d) **Vulnerabilidades de terceras partes:** que un atacante pueda explotar vulnerabilidades existentes en el software de terceras partes utilizado por el sistema de virtualización (sistema operativo del host, drivers de los dispositivos físicos, etc.), tomar control del sistema y comprometerlo.

e) **Compromiso del sistema de virtualización:** que un fallo en los mecanismos de seguridad del sistema de virtualización pueda causar una intrusión en el sistema, con la consecuente alteración malintencionada de cualquiera de sus componentes.

f) **Compromiso de la plataforma:** que un atacante pueda acceder a la plataforma de una manera no controlada por el sistema de virtualización, modificar el firmware o el software del sistema, y comprometer tanto el sistema de virtualización como la plataforma subyacente.

g) **Acceso no autorizado:** que un atacante pueda conseguir acceso a la interfaz de gestión del sistema, modificar su configuración de seguridad y comprometer así el sistema de virtualización.

h) **Cifrado débil:** que un atacante pueda romper el cifrado del sistema, debido al uso de un cifrado débil porque el sistema no proporcione suficiente entropía para implementar correctamente las funciones criptográficas.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS) . VIRTUALIZACIÓN DE SERVIDOR

25. A continuación, se recogen los requisitos que deben cumplir los productos de la familia Virtualización para el caso de uso 1: Herramientas de virtualización de Servidor.

4.1 PERFIL DE PROTECCIÓN COMMON CRITERIA

26. **REQ. 1**. Los productos deberán estar certificados con el siguiente perfil de protección de acuerdo a la norma Common Criteria:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Virtualization	*1.0*	*17/11/2016*	*NIAP*
Protection Profile for Server Virtualization	*1.1*	*14/09/2015*	*NIAP*

Tabla 1. Perfiles de Protección.

27. **REQ. 2**. En caso de que el producto no esté certificado contra ninguno de los perfiles anteriores, debe disponer de una declaración de seguridad (*Security Target*) certificada con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**. La declaración de seguridad debe implementar los SFR (*Security Functional Requirements*) apropiados para satisfacer, al menos, los Objetivos de Seguridad que se recogen en la siguiente tabla:

OBJETIVO	DESCRIPCIÓN
[VIRTUALIZACIÓN] PROTECCIÓN DE LAS VMS	El producto debe proporcionar los mecanismos apropiados para aislar las VMs, de forma que la ejecución de una VM no interfiera de ninguna forma en otras VMs.
[VIRTUALIZACIÓN] CONTROL DEL FLUJO DE INFORMACIÓN	El producto debe proporcionar los mecanismos apropiados para garantizar que el tráfico destinado a una VM, sólo es entregado a esa VM a través del interfaz físico correcto.
[AUDITORÍA] REGISTRO DE EVENTOS	El producto debe tener la capacidad de detectar los eventos relevantes que ocurren en el sistema, y registrarlos con la información adecuada en los registros de auditoría, para su posterior análisis.
[AUDITORÍA] PROTECCIÓN DE LOS REGISTROS	El producto debe proteger los registros de auditoría almacenados o trasmitidos, de accesos no autorizados.
[GESTIÓN DE LA SEGURIDAD] FUNCIONALIDAD	El producto debe proporcionar características de gestión que permitan el control de sus funciones y datos, asegurándose de que solo los administradores con los privilegios adecuados puedan ejercer dicho control.
[GESTIÓN DE LA SEGURIDAD] PERMISOS Y ROLES	El producto debe permitir la definición de perfiles de administración (roles), y la asignación de distintas funciones de gestión a cada perfil (*separation of duties*).
[PROTECCIÓN DE LAS COMUNICACIONES]	El producto debe proteger la confidencialidad y la integridad de los datos transmitidos entre los componentes del producto, y entre el producto y los administradores u otras entidades IT externas.
[CONTROL DE ACCESO] AUTENTICACIÓN	El producto debe identificar de forma única a los usuarios y administradores, y autenticarlos antes de permitirles acceso las funciones y datos del producto.
[CONTROL DE ACCESO] CONTROL DE SESIONES	El producto debe implementar mecanismos que permitan denegar o suspender las sesiones establecidas por los usuarios y administradores.
[CONTROL DE ACCESO] POLÍTICA DE CONTRASEÑAS	El producto debe implementar una política de contraseñas que establezca unas características mínimas de complejidad y longitud.

Tabla 2. Objetivos de Seguridad.

4.2 SOPORTE CRIPTOGRÁFICO

28. **REQ. 3**. En caso de que el producto utilice algoritmos y funciones criptográficas, debe soportar el uso de aquellas aceptadas para nivel Alto del ENS según la guía

CCN-STIC-807, así como proporcionar capacidades de configuración que permitan obligar al uso de estos algoritmos exclusivamente.

29. **REQ. 4**. El producto debe disponer de un mecanismo para, en caso necesario, proporcionar entropía a las máquinas virtuales (VMs). Deberá asegurar que esta entropía se suministra de forma independiente entre VMs, es decir, que la provisión de entropía a una VM no afecta a la calidad de la entropía proporcionada a otra VM en la misma plataforma.
30. **REQ. 5**. El producto debe soportar el uso de mecanismos criptográficos que proporcionen una fortaleza equivalente a 128 bits o superior.

4.3 AUDITORÍA

31. **REQ. 6**. El producto debe registrar, al menos, los siguientes eventos en los registros de auditoría: arranque/parada de la función de auditoría, uso de los mecanismos de identificación y autenticación, y acciones administrativas, incluyendo cualquier modificación de la configuración del sistema.
32. **REQ. 7**. Cada registro contendrá, al menos, los siguientes datos: fecha/hora del evento, identidad del sujeto (si procede) y resultado del evento (éxito o fallo).

5. ABREVIATURAS

CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
CPU	*Central Processing Unit*
EAL	*Evaluation Assurance Level*
ENS	Esquema Nacional de Seguridad
NIAP	*National Information Assurance Partnership*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*
SO	Sistema Operativo
VM	*Virtual Machine*
VMM	*Virtual Machine Monitor*