centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo F.7-M: Virtualización

Noviembre de 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.01.03 14:53:00 +01'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2022
NIPO: 083-22-102-1

Fecha de Edición: noviembre de 2022

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 y Servicios STIC (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) para categoría MEDIA**. 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:
9. Puede reducir la superficie de ataque considerablemente.
10. Permite encapsular SO heredados que no puedan alcanzar una protección adecuada por ellos mismos.
11. 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.
12. 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

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

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

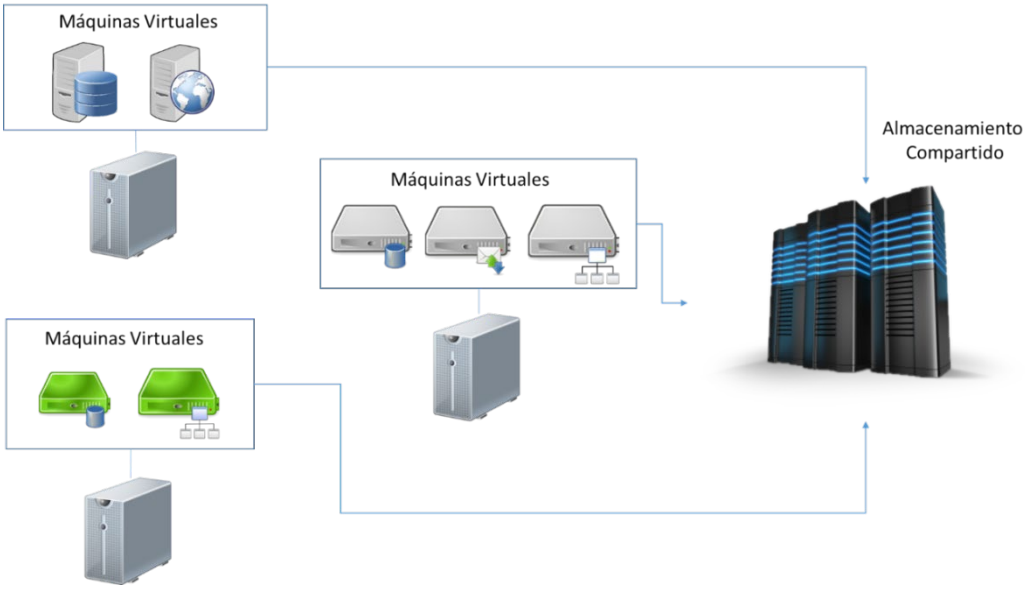

Figura 1. Ejemplo de Caso de Uso: Virtualización de Servidores.

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

19. 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.

20. 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:

    - **Protección física.** El producto debe estar protegido físicamente por su entorno operacional y no sujeto a ataques físicos que puedan comprometer su seguridad o interferir en su correcta operación. En caso de productos software, esta hipótesis aplica a la plataforma física sobre la que se ejecuta el producto.

    - **Administración confiable**. Los administradores son miembros de plena confianza y velan por los mejores intereses en materia de seguridad de la organización. Dichas personas deben estar debidamente capacitadas y carecer de cualquier intención maliciosa o conflicto de intereses al administrar el producto.

    - **Actualizaciones periódicas.** El *firmware/software* del producto es actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.

    - **Funcionalidad limitada.** El producto solo debe proporcionar la funcionalidad de *Virtualización* como función principal y no debe proporcionar ninguna otra funcionalidad o servicio.

- **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.
- **Plataforma confiable**. En caso de tratarse de un producto software, este se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución que la plataforma proporcione.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

21. 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 CERTIFICACIÓN LINCE

22. Para que un producto de esta familia pueda ser incluido en el CPSTIC bajo la categorización de ENS Medio, deberá disponer de una Certificación Nacional Esencial de Seguridad (LINCE)[1] que incluya los RFS reflejados en el apartado 4, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.
23. El alcance de la evaluación deberá incluir el módulo de evaluación básico de 25 días de esfuerzo y el Módulo de Evaluación Criptográfica (MEC). El Módulo de Revisión de Código Fuente (MCF) será opcional.
24. En caso de estimarse que el esfuerzo de evaluación de los requisitos incluidos en el apartado 4 excede de los días de esfuerzo determinados dentro de la metodología LINCE, se contempla la posibilidad de realizar una Evaluación STIC Complementaria que incluya las pruebas que no han podido ser encajadas en el mencionado periodo.

[1] Toda la información relativa a esta metodología se encuentra disponible en la web del Organismo de Certificación (https://oc.ccn.cni.es)

3. ANÁLISIS DE AMENAZAS

3.1 ACTIVOS SENSIBLES A PROTEGER

25. Los recursos que deben protegerse mediante el uso de estos productos son:

- **AC.Administración**. Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos, que debe ser protegida en Confidencialidad, Trazabilidad, Autenticidad e Integridad.
- **AC.PSS.** Datos de configuración, registros auditoría y [***asignación**: listado de datos definidos por el fabricante]* que deben ser protegidos en Integridad.
- **AC.PSC**. [**selección**: credenciales; claves; [**asignación**: *listado de datos definidos por el fabricante*] que deben ser protegidos en Confidencialidad e Integridad.
- **AC.Actualizaciones**. Actualizaciones del producto susceptibles de afectar a su configuración y funcionalidad, que deben ser protegidos en Integridad y Autenticidad.
- **AC.Comunicaciones.** Comunicaciones del producto, establecidas entre sus propios componentes y con [**asignación**: *listado de entidades autorizadas*] que deben ser protegidas en Confidencialidad, Integridad y Autenticidad.

3.2 AMENAZAS

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

- **A.NOAUT Acceso no autorizado de administrador:** Un atacante puede obtener un acceso de administración no autorizado haciéndose pasar por un administrador ante el producto, haciéndose pasar por el producto ante un administrador, reproduciendo una sesión de administración, o realizando ataques del hombre en medio.
- **A.CRYPTO Mecanismos criptográficos débiles:** Utilización en el producto de mecanismos criptográficos o longitudes de clave débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
- **A.COM Protocolos de comunicación no autorizados:** Utilización de protocolos no autorizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones críticas del producto.
- **A.AUD Actividades no detectadas:** Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador.

- **A.PSC Compromiso de parámetros de seguridad críticos:** Un atacante puede comprometer los parámetros de seguridad críticos y acceder de forma continuada al producto y a sus datos críticos.
- **A.FUN Fallo de las funcionalidades de seguridad:** Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad declaradas del producto y podría acceder, cambiar o modificar información, funcionalidades de seguridad o tráfico de red en el producto.
- **A.NOAUTUSR Acceso no autorizado de usuario:** Un atacante puede obtener un acceso no autorizado haciéndose pasar por un usuario ante el producto, haciéndose pasar por el producto ante un usuario, reproduciendo una sesión de usuario, o realizando ataques del hombre en medio.
- **A.CRE Compromiso de credenciales:** Un atacante puede aprovecharse del uso credenciales débiles o desprotegidas, para ganar acceso privilegiado al producto.

3.3 TRAZABILIDAD AMENAZAS/REQUISITOS DE SEGURIDAD

27. En la siguiente tabla se trazan que Requisitos Fundamentales de Seguridad definidos en el apartado 4 cubren las amenazas definidas:

	A.NOAUT	A.CRYPTO	A.COM	A.AUD	A.PSC	A.NOAUTUSR	A.CRE	A.FUN
ADM.1	X							
ADM2	X							
ADM.3	X							
IAU.1	X					X		
IAU.2							X	
IAU.3							X	
IAU.4	X							
COM.1		X	X					
COM.2			X					
COM.4		X	X					
AUD.1				X				
AUD.2				X				

	A.NOAUT	A.CRYPTO	A.COM	A.AUD	A.PSC	A.NOAUTUSR	A.CRE	A.FUN
AUD.3				X				
AUD.4				X				
AUD.5				X				
PSC.1					X			
CIF.1		X	X					
CIF.2		X	X					
VIR.1								X
VIR.2								X
VIR.3								X

4. REQUISITOS DE SEGURIDAD

28. 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.

29. La convención utilizada en las descripciones de los RFS es la siguiente:

- Selección: se deberá seleccionar al menos una opción de las indicadas en el RFS y se incluirá en la declaración de seguridad. Ejemplo:

  RFS: Administración del producto [**selección***: local; remota*]

  DS: Administración del producto local y remota

- Asignación: se deberá especificar el listado de opciones que sean de aplicación al TOE (podría no haber ninguna). Ejemplo:

  RFS: El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación:** otros usuarios del producto] antes de otorgar acceso.

  DS: El TOE deberá identificar y autenticar a cada usuario administrador, auditor y usuario avanzado antes de otorgar acceso.

4.1 ADMINISTRACIÓN CONFIABLE

30. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

31. **ADM.1** El TOE debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.

32. **ADM.2** El TOE debe ser capaz de realizar la gestión de las siguientes funcionalidades:

- Administración del producto [**selección**: *local; remota*].
- Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.
- [**asignación**: otras funcionalidades administrables del producto].

33. **ADM.3** El TOE deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones descritas en **ADM.2**.

> Nota de aplicación: en el caso de que existan distintos tipos de administrador, cada uno de ellos con distintos permisos, deberá probarse que únicamente pueden realizar aquellas funcionalidades para las que tengan permiso.

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

34. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

35. **IAU.1** El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación**: *otros usuarios del producto*] antes de otorgar acceso, salvo para las siguientes funcionalidades [**asignación**: *listado funcionalidades*].

36. **IAU.2** El TOE deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.

37. **IAU.3** El TOE debe disponer de la capacidad de gestión de las contraseñas:

    a) La contraseña debe poder configurarse con una longitud mínima o igual a 12 caracteres.

    b) La contraseña debe ser capaz de componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “].

> Nota de aplicación: este requisito podría ser modificado en el caso de que el TOE implemente otros mecanismos de autenticación.

38. **IAU.4** El TOE debe [**selección***: bloquear; cerrar*] la sesión de un usuario después de [***asignación****: tiempo de inactividad*] de inactividad.

4.3 CANALES SEGUROS

39. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

40. **COM.1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas: [**selección***: servidor de auditoría;* [***asignación****: otras entidades*]] o entre distintas partes del producto, usando [**selección***: IPSec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación****: listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

41. **COM.2** El TOE debe permitir que los canales de comunicación definidos en **COM.1** sean iniciados por él mismo o por las entidades autorizadas.

42. **COM.4** Protección de la información del canal de administración. El TOE deberá establecer canales seguros cuando intercambie información con el administrador remoto, usando [**selección**: *IPsec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación****: listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

4.4 AUDITORÍA

43. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

44. **AUD.1** El TOE debe generar registros de auditoría cuando se produzca alguno de los siguientes eventos:
    a) Al inicio y finalización de las funciones de auditoría.
    b) *Login* y *logout* de usuarios registrados.
    c) Cambios en las credenciales de usuarios.
    d) Cambios en la configuración del producto [**asignación**: *listado de cambios*].
    e) Eventos relativos a la funcionalidad del producto [**asignación:** *listado de eventos*].
    f) Si el TOE gestiona claves criptográficas, [**selección:** generación; importación; cambio; eliminación de claves criptográficas; ningún otro].
45. **AUD.2** 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.
46. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:
    a) Lectura: usuarios autorizados.
    b) Modificación: ningún usuario.
    c) Borrado: [**selección**: solo administradores; ningún usuario]
47. **AUD.4** El TOE debe ser capaz de almacenar en sí mismo la información de auditoría generada y [**selección**: transmitir la información de auditoría generada a una entidad externa utilizando un canal seguro COM.1; no transmitir la información de auditoría generada].
48. **AUD.5** El TOE deberá [**selección**: sobreescribir los registros siguiendo el criterio de mayor antigüedad; enviar a una entidad externa y eliminar; otra opción validada por el CPSTIC] en el caso de que el espacio para almacenamiento de los registros alcance su límite.

4.5 CRIPTOGRAFÍA

49. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
50. **CIF.1** El TOE permitirá exclusivamente el empleo de mecanismos criptográficos: [***asignación****: listado de mecanismos*] autorizados de acuerdo a lo establecido en la guía CCN-STIC-807. La fortaleza de clave empleada será la indicada en esa guía para Categoría MEDIA del ENS, y de acuerdo al nivel de amenaza establecido.
51. **CIF.2.** Generador de bits aleatorios. En caso de suministrar un servicio de generación de bits aleatorios (RBG[2]) determinísticos, el producto deberá:

[2] *Random Bit Generator*

- Utilizar [**selección:** *Hash_DRBG (any), HMAC_DRBG (any)* o *CTR_DRBG (AES)*].
- Usar una semilla de, al menos, una Fuente de entropía que acumule entropía [selección: de una o varias fuentes; una Fuente de entropía estudiada], con un mínimo de bits de entropía al menos igual a la mayor Fortaleza de seguridad de las claves y hashes que generará, de acuerdo a la ISO/IEC 18031:2011.

4.6 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

52. **PSC.1** En el caso en que el TOE almacene [***selección**: credenciales; claves privadas; [**asignación**: otros parámetros de seguridad críticos*] estos no deberán almacenarse en claro, sino que se utilizarán mecanismos de protección criptológica que cumplan con CIF.1.

4.7 VIRTUALIZACIÓN

53. **VIR.1** El TOE 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.
54. **VIR.2** El TOE 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.
55. **VIR.3** El TOE 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.

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
TOE	*Target of Evaluation*
VM	*Virtual Machine*
VMM	*Virtual Machine Monitor*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL