centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC-
Anexo F.12: Infraestructura de escritorio virtual (VDI)

Junio 2021

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

NIPO: 083-21-130-1

Fecha de Edición: junio de 2021

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 **Infraestructura de Escritorio Virtual (VDI)** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos y Servicios 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 para los que sea de aplicación el **Esquema Nacional de Seguridad (ENS), categoría ALTA**. 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 **Infraestructura de Escritorio Virtual (VDI)** 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. La **Infraestructura de Escritorio Virtual (VDI)** es una tecnología que permite a los usuarios disponer de un entorno de escritorio, accesible de forma remota a través de un dispositivo cliente. El usuario puede manejar un escritorio completo o una aplicación, de la misma forma que si se estuviese ejecutando en su propio equipo.
7. VDI proporciona flexibilidad y eficiencia a las organizaciones a la hora de gestionar los recursos TI. También da facilidades a los empleados a la hora de desarrollar su trabajo, independientemente de su ubicación física.
8. Los escritorios se ejecutan en máquinas virtuales alojadas en un servidor. Estas máquinas virtuales están asociadas a un hipervisor, que es el componente encargado de crearlas y gestionarlas. A este conjunto de elementos se le denomina **capa de recursos**. Normalmente esta capa de recursos no forma parte de la solución VDI, pudiendo usarse un sistema de virtualización de servidor ya existente en la organización, o de cualquier fabricante. Generalmente, la solución VDI instalará un componente tipo agente para poder establecer la comunicación entre las máquinas y aplicaciones virtuales y el cliente remoto.
9. A los componentes encargados de gestionar la capa de recursos y entregar los escritorios y aplicaciones a los usuarios remotos se les denomina **capa de control**. Sus componentes principales son los siguientes:
    a) Un ***gateway***, encargado de autenticar a los usuarios y establecer las conexiones seguras entre los usuarios y los recursos.
    b) Un **controlador**, encargado de comunicarse con la capa de recursos (habitualmente con el hipervisor), para distribuir y gestionar las máquinas virtuales. En algunos productos, las funciones de gateway y de controlador las realiza un mismo componente.
    c) Una o varias **bases de datos**, que almacenan información sobre usuarios o licencias, entre otros.
10. El usuario accederá a los recursos proporcionados por el sistema VDI a través de un dispositivo cliente que generalmente tendrá un agente instalado mediante el cual se iniciará la conexión con el escritorio o aplicación virtual asignado por el producto VDI. Este dispositivo podrá ser un equipo con un sistema operativo comercial, un cliente ligero (*thin client*) con menos recursos y un sistema operativo más reducido, o también un dispositivo *zero client,* que no llega a tener sistema operativo, y utiliza un firmware específicamente diseñado para establecer la conexión con el sistema VDI.
11. El dispositivo cliente y el servidor donde se ejecuta el escritorio o aplicación virtual intercambian datos a través de un protocolo de presentación. Este protocolo es el encargado de transmitir toda la información necesaria para que

el usuario pueda manejar el escritorio o aplicación. Dicha información incluye datos multimedia, de teclado y de ratón, entre otros. La comunicación debe estar protegida con mecanismos de cifrado, para evitar la modificación de los datos y el acceso no autorizado.

12. El uso de VDI permite proporcionar solo los recursos necesarios para que el usuario desempeñe sus funciones. Además, al ejecutarse el escritorio en una máquina virtual, facilita el aislamiento en caso de infección por *malware*, permitiendo sustituir la máquina de forma sencilla.

2.2 CASOS DE USO

13. En base a las funcionalidades y características del producto, se contemplan dos (2) casos de uso para esta familia de productos, tal y como se definen a continuación.

2.2.1. CASO DE USO 1. ESCRITORIOS VIRTUALES

14. El producto proporciona acceso a entornos de escritorio completos. Los usuarios previamente autenticados pueden manejar estos entornos desde cualquier ubicación, a través de un dispositivo cliente.

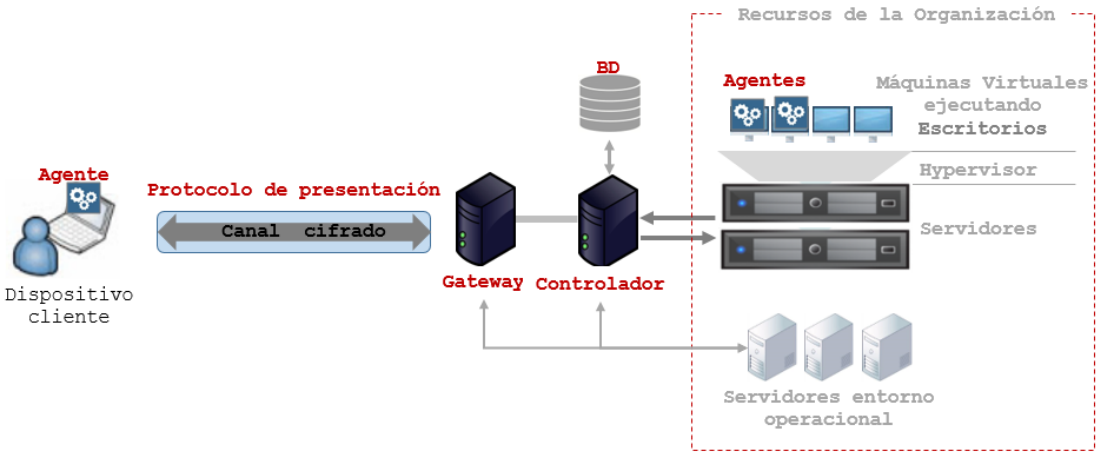

Figura 1: Arquitectura VDI con escritorios virtuales

2.2.2. CASO DE USO 2. ESCRITORIOS Y APLICACIONES VIRTUALES

15. El producto proporciona acceso a entornos de escritorio completos, y también a aplicaciones individuales. Al igual que en el caso de uso anterior, los usuarios previamente autenticados pueden acceder a estos recursos desde cualquier ubicación, a través de un dispositivo cliente.

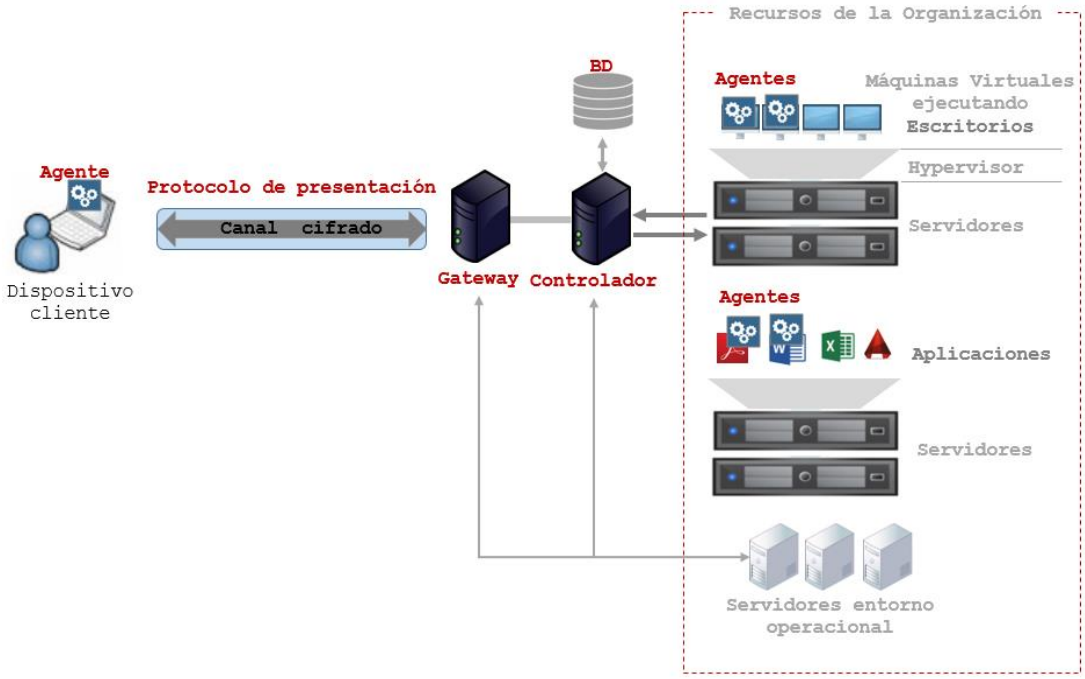

Figura 2: Arquitectura VDI con escritorios virtuales y aplicaciones

2.3 ENTORNO DE USO

16. Estos productos son usados por organizaciones de mediano y gran tamaño para proporcionar acceso remoto a sus recursos, así como un entorno de trabajo remoto para sus empleados.

17. Para la utilización en condiciones óptimas de seguridad de las **Infraestructuras de Escritorio Virtual (VDI)**, es necesario que se integren en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

    - **Plataforma segura:** El producto se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.
    - **Protección física:** Los componentes del producto deberán instalarse en un área donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.
    - **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.
    - **Flujo de información:** El intercambio de información entre el escritorio virtual o aplicación y el cliente, sólo podrá realizarse a través del producto, utilizando los mecanismos criptográficos necesarios para proteger la confidencialidad e integridad de la información.

- **Actualizaciones periódicas:** El *software* del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **Acceso:** El producto tiene acceso a todos los datos del sistema necesarios para llevar a cabo todas sus funciones.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

18. Estos productos constan de varios componentes, que generalmente se presentan en formato *software*, y que se ejecutan sobre plataformas hardware de propósito general con un sistema operativo compatible. Normalmente, estos componentes requieren comunicarse con otros componentes que no forman parte de la solución, pero sí deben formar parte del entorno operativo, como servidores de autenticación, hipervisores para gestionar las máquinas virtuales, bases de datos, etc.

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 TIC (Tecnologías de la Información y de las Comunicaciones).
20. En el ámbito de CC se definen un conjunto de objetivos y requisitos de seguridad, tanto funcionales (*SFR, Security Functional Requirements*) como de evaluación (*SAR, Security Assurance Requirements*), independientes de la implantación, que cada producto incluirá dentro de su declaración de seguridad (*ST, Security Target*).
21. **Los productos dentro de esta familia, deberán disponer de una declaración de seguridad (ST) certificada con un nivel de confianza EAL2 o superior (*Evaluation Assurance Level*), que contenga los SFR indicados en el apartado 4.**
22. En caso de que alguno de los requisitos indicados en dicho apartado 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

23. Los recursos que es necesario proteger mediante el uso de esta familia de productos, incluyen:

- **Comunicación** entre el cliente remoto y el escritorio virtual o aplicación, de forma que se proteja la integridad y confidencialidad de los datos transmitidos.
- **Información** de los usuarios del producto.
- **Recursos** ofrecidos por el producto (escritorios y aplicaciones virtuales), de forma que no sean accedidos por usuarios no autorizados.
- **Plataforma** sobre la que se ejecuta el producto, de forma que ningún usuario o *software* pueda afectar a la misma.
- **Funcionalidad** del producto y datos de configuración y auditoría generados por éste.

3.2 AMENAZAS

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

- **A.RED. Ataque a la red.** Un atacante, desde dentro o desde fuera de la red, podría acceder y/o modificar la información intercambiada entre el producto y otras entidades autorizadas o entre los distintos módulos del producto.
- **A.LOCAL. Ataque local.** Un atacante podría actuar a través de *software* no privilegiado ejecutado en la misma plataforma de computación donde se ejecuta el producto. Los atacantes podrían modificar de forma maliciosa los ficheros o comunicaciones que utiliza el producto.
- **A.REST. Acceso a información almacenada.** Un atacante podría acceder a información sensible almacenada en la plataforma en la que se instala y ejecuta el producto.
- **A. SEG. Acceso a las funciones de seguridad.** Un atacante podría acceder y modificar las funciones y datos de seguridad del producto.
- **A.NODET. Actividad no detectada.** Un atacante podría acceder, cambiar o modificar la funcionalidad de seguridad de la herramienta sin que esto sea apreciado por el administrador.
- **A.VDI. Acceso no autorizado a recursos**. Un usuario podría acceder a recursos para los que no posee autorización, como pueden ser escritorios, aplicaciones, información almacenada en ellos o información en tránsito.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

25. 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.
26. Los requisitos que mencionen el uso de aplicaciones virtuales, **sólo aplicarán al caso de uso 2**.

4.1 ADMINISTRACIÓN CONFIABLE

27. Estas funcionalidades de seguridad mitigan la amenaza (A.SEG). **Podrán ser cubiertas por el producto o por su entorno operacional.**
28. **ADM.1** El producto debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.
29. **ADM.2** El producto debe ser capaz de realizar la gestión de las siguientes funcionalidades:
    - Administración del producto de forma local y remota.
    - Configuración del tiempo de terminación de sesión o bloqueo, al detectar inactividad.
    - Otros parámetros de configuración del producto.

    Nota de aplicación: En este punto se espera que el fabricante enumere todas las tareas de administración que puedan ser realizadas.
30. **ADM.3** El producto deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones anteriormente descritas (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 funcionales para las que tengan permiso.

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

31. Estas funcionalidades de seguridad mitigan la amenaza (A.REST, A.SEG). **Podrán ser cubiertas por el producto o por su entorno operacional.**
32. **Estos requisitos aplican tanto a los administradores del producto, como a los usuarios de escritorios virtuales y aplicaciones publicadas.**
33. **IAU.1.** El producto deberá identificar y autenticar a cada usuario antes de otorgar acceso.
34. **IAU.2.** El producto deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.

35. **IAU.3.** El producto deberá proteger de lectura y modificación no autorizada las credenciales de autenticación.
36. **IAU.4.** El producto deberá disponer de la capacidad de gestión de las contraseñas:
    a) La contraseña debe poder configurarse con una longitud mínima o igual a 9 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 producto implemente otros mecanismos de autenticación. Será estudiado caso por caso.
37. **IAU.5.** El producto debe bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad.
38. **IAU.6.** En caso de que el producto realice la autenticación de usuarios, deberá proporcionar una autenticación multi-factor utilizando usuario y contraseña y, al menos, un factor de la categoría “*algo que se tiene*” o de la categoría “*algo que se es*” o permitir integrarse con herramientas que provean esta funcionalidad.

4.3 AUDITORÍA

39. Estas funcionalidades de seguridad mitigan la amenaza (A.NODET).
40. **AUD.1.** El producto deberá generar registros de auditoría al comienzo y finalización de las funciones de auditoría y cuando se produzca alguno de los siguientes eventos:
    a) *Login* y *logout* de personal autorizado.
    b) Cambios en las credenciales de usuarios.
    c) Cambios en la configuración del producto.
    d) Eventos relativos a la funcionalidad del producto
41. **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 (si aplica).
42. **AUD.3.** A los registros de auditoría se aplicará la siguiente política de acceso:
    a) Lectura: usuarios autorizados.
    b) Modificación: ningún usuario.
    c) Borrado: solo administradores.
43. **AUD.4.** El producto debe ser capaz de almacenar la información de auditoría generada en sí mismo o en una entidad externa.

44. **AUD.5.** El producto debe ser capaz de eliminar o sobrescribir registros de auditoría anteriores cuando el espacio de almacenamiento esté lleno.

4.4 CANAL SEGURO

45. Estas funcionalidades de seguridad mitigan la amenaza (A.RED).
46. **COM.1.** El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas o entre distintas partes del producto empleando funciones, algoritmos y protocolos que estén de acuerdo a lo establecido en la guía CCN-STIC-807 (p.ej.: HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, etc.).
47. **COM.2** El TOE debe permitir que estos canales de comunicación seguros sean iniciados por él mismo o por entidades autorizadas.
48. **COM.3** El producto hará uso de certificados digitales para la autenticación cuando utilice cualquiera de estos protocolos.

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

49. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL, A.SEG).
50. **ACT.1** El producto ofrecerá la posibilidad de consultar la versión actual del firmware/software, iniciar actualizaciones manualmente y comprobar si existen nuevas actualizaciones disponibles.
51. **ACT.2** El producto deberá ofrecer mecanismos, conforme a la criptografía de empleo en el ENS, a través de hashes o firma digital para autenticar las actualizaciones de *firmware/software* antes de instalarlas.
52. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.
53. **ACT.5** El producto deberá estar empaquetado de forma que, si se elimina, no deje rastro de su instalación (excepto por configuraciones y ficheros de salida o auditoría).
54. **ACT.6** El producto no descargará ni modificará su propio código binario.
55. **ACT.7** El producto solamente utilizará las bibliotecas de terceras partes declaradas por el fabricante.
56. **Nota de aplicación**: Los requisitos ACT.5, ACT.6 y ACT.7 serán de aplicación al agente, cuando éste sea desplegado el Dispositivo Cliente.

4.6 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

57. Estas funcionalidades de seguridad mitigan la amenaza (A.REST). **Podrán ser cubiertas por el producto o por su entorno operacional.**

58. **CRD.1.** En el caso en que el producto almacene credenciales y/o datos sensibles, éstos no deberán almacenarse en claro.
59. **CRD.2.** En el caso en el que el producto utilice sus propias credenciales de acceso, el producto obligará al cambio/establecimiento de credenciales cuando el acceso se realice utilizando credenciales por defecto o el usuario no tenga asignadas credenciales.

4.7 REQUISITOS CRIPTOGRÁFICOS

60. Estas funcionalidades de seguridad mitigan las amenazas (A.RED, A.REST).
61. **CIF.1** El TOE permitirá exclusivamente el empleo de funciones, algoritmos y protocolos criptográficos que estén incluidas entre las autorizadas para categoría ALTA del ENS, de acuerdo a lo establecido en la guía CCN-STIC-807.
62. **CIF.2** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).

4.8 INFRAESTRUCTURA DE ESCRITORIO VIRTUAL (VDI)

63. Estas funcionalidades de seguridad mitigan la amenaza (A.VDI).
64. **VDI.1.** El administrador deberá poder configurar una política de control de acceso a escritorios virtuales que permita el acceso a un escritorio virtual solo a los usuarios autorizados.
65. **VDI.2.** El administrador deberá poder configurar una política de control de acceso a aplicaciones publicadas que permita el acceso a una aplicación publicada solo a los usuarios autorizados.
66. **VDI.3.** El administrador deberá poder configurar una política de compartición de datos entre escritorios virtuales o aplicaciones publicadas y el equipo de usuario (*endpoint*). Existirá una política por defecto, que no permita ninguna compartición de datos. El administrador podrá permitir solo a usuarios autorizados:
    - Compartir datos a través de los portapapeles (*clipboard*).
    - Acceso desde el escritorio virtual o aplicación, a unidades mapeadas del equipo de usuario.
    - Acceso desde el escritorio virtual o aplicación, a dispositivos USB, lectores CD/DVD u otros dispositivos externos, conectados en el equipo de usuario.
    - Cualquier otro mecanismo que permita una compartición de datos entre el equipo de usuario y el escritorio virtual o la aplicación publicada.
67. **VDI.4.** El producto deberá establecer un canal seguro entre el usuario remoto y la máquina virtual que ejecuta su entorno de escritorio, proporcionando autenticación, protección de la confidencialidad y de la integridad. Para ello empleará funciones, algoritmos y protocolos que estén de acuerdo a lo

establecido en la guía CCN-STIC-807 (p.ej.: HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, etc.).

68. **VDI.5.** El producto debe monitorizar las sesiones activas de usuarios y permitir al administrador finalizar una sesión determinada.

4.9 NOTAS DE APLICACIÓN

69. En caso de que el producto no implemente la funcionalidad a la que aplica alguno de los requisitos anteriores (o algunas partes de ellos), y ésta sea proporcionada por el entorno operacional, el fabricante deberá indicarlo en la declaración de seguridad o justificarlo debidamente. En este caso, se evaluará si dada la misión y capacidades del producto, se puede considerar que el requisito ***no aplica***.

70. Lo anterior no es válido en caso de que tal funcionalidad solicitada en un requisito, sea proporcionada por un componente del producto que no forma parte de la configuración evaluada. En este caso ***sí aplica***, y el fabricante deberá demostrar el correcto cumplimiento del requisito por parte del producto.

5. ABREVIATURAS

CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de Información y las Comunicaciones
EAL	*Evaluation Assurance Level*
ENS	Esquema Nacional de Seguridad
NIAP	*National Information Assurance Partnership*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*
URL	*Uniform Resource Locator*

PUBLICACIONES DE DEFENSA

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