centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

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

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 criptológico nacional

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 14:57:22 +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* ***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), 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 ***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.

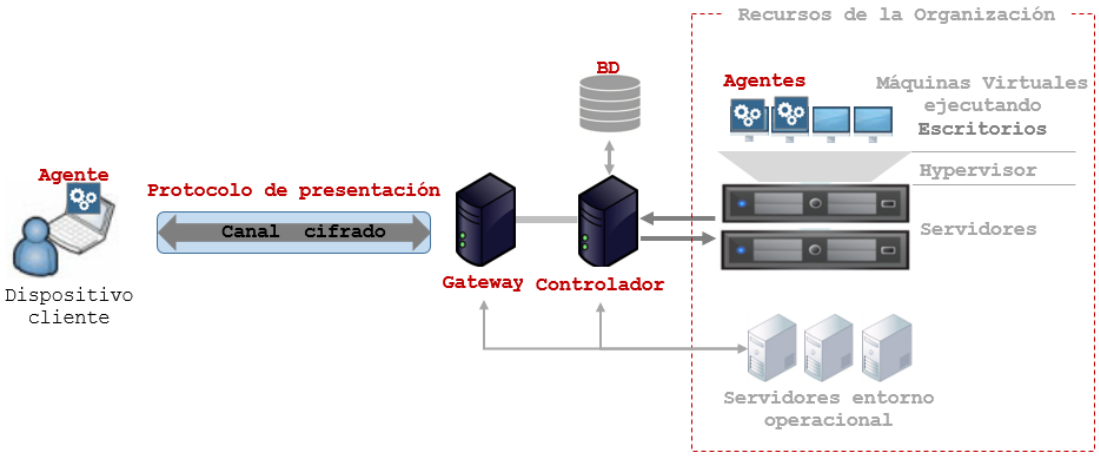

Figura 1: Arquitectura VDI con escritorios virtuales

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.

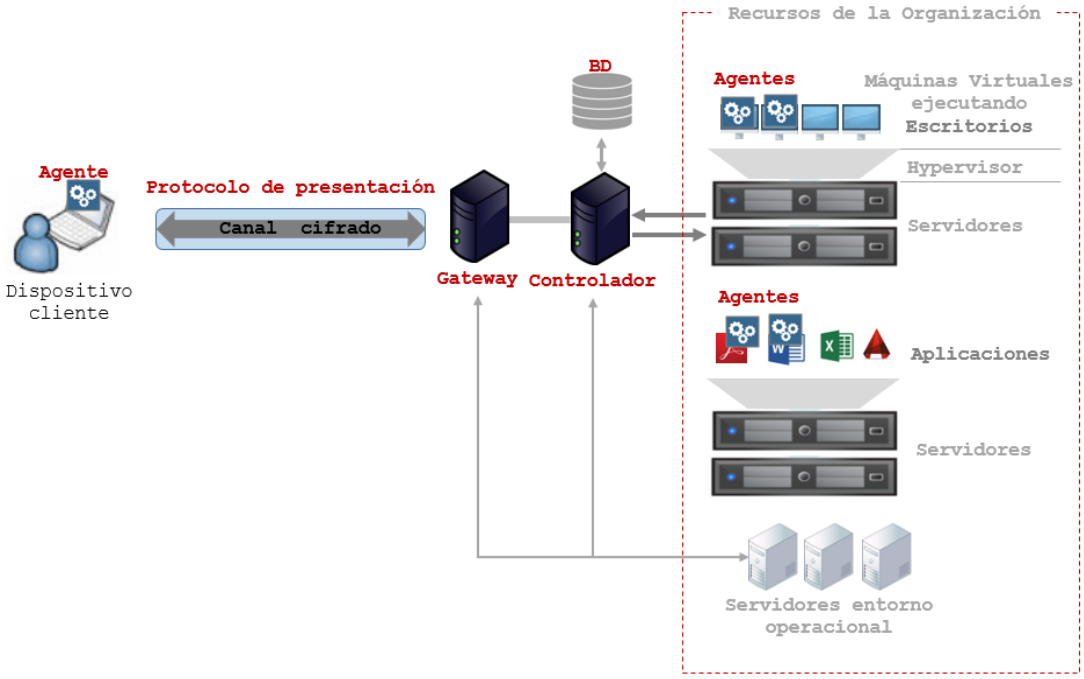

Figura 2: Arquitectura VDI con escritorios virtuales y aplicaciones

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

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:

18. **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.

19. **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.

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

21. **Funcionalidad limitada.** El producto solo debe proporcionar la funcionalidad de **Infraestructura de Escritorio Virtual** como función principal y no debe proporcionar ninguna otra funcionalidad o servicio.

22. **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.

23. **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

24. 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 CERTIFICACIÓN LINCE

25. Para que un producto de esta familia pueda ser incluido en el CPSTIC bajo la categorización de ENS Categoría Media, deberá disponer de una Certificación Nacional Esencial de Seguridad (LINCE)[1] que incluya los RFS reflejados en el apartado 4, evaluados considerando el problema de seguridad definido en el presente documento.

26. El alcance de la evaluación deberá incluir el módulo de evaluación básico de 25 días de esfuerzo. Los Módulos de Revisión de Código Fuente (MCF) y de Evaluación Criptográfica (MEC) serán opcionales.

[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

27. 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

28. 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.ACT Actualización maliciosa:** un atacante puede realizar una actualización maliciosa que comprometa las funcionalidades 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.INT Compromiso de la integridad del software/firmware:** Un atacante puede intentar comprometer la integridad del producto a través de un software sin privilegios ejecutado en la misma plataforma en la que se ejecuta el producto.
- **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.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.
- **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.

3.3 TRAZABILIDAD AMENAZAS/REQUISITOS DE SEGURIDAD

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.ACT	A.AUD	A.INT	A.PSC	A.NOAUTUSR	A.CRE	A.VDI
ADM.1	X									
ADM2	X									
ADM.3	X									
IAU.1	X							X		
IAU.1								X		
IAU.2									X	
IAU.3									X	

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.INT	A.PSC	A.NOAUTUSR	A.CRE	A.VDI
IAU.4	X									
IAU.5	X									
COM.1		X	X							
COM.2			X							
COM.3			X							
COM.4		X	X							
ACT.1				X						
ACT.2				X						
ACT.3				X						
ACT.4				X						
ACT.5				X						
AUD.1					X					
AUD.2					X					
AUD.3					X					
AUD.4					X					
AUD.5					X					
EXP.3						X				
PSC.1							X			
CIF.1		X	X							
VDI.1										X
VDI.2										X
VDI.3										X
VDI.4										X
VDI.5										X
VDI.6										X

4. REQUISITOS DE SEGURIDAD

29. 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.

30. 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.

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

4.1 ADMINISTRACIÓN CONFIABLE

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

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

34. **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].

35. **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

36. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional. Estos requisitos aplican tanto a los administradores del producto, como a los usuarios de escritorios virtuales y aplicaciones publicadas.

37. **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*].

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

39. **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.

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

41. **IAU.5** Cuando el acceso se realice utilizando credenciales por defecto o el usuario no tenga asignadas credenciales, el TOE obligará al [**selección***: cambio; establecimiento*] de credenciales en el siguiente acceso.

4.3 AUDITORÍA

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

43. **AUD.1** El producto 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].

44. **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.

45. **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]

46. **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].

47. **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.

4.4 CANALES SEGUROS

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

49. **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*].

50. **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.

51. **COM.3** El TOE hará uso de certificados digitales para la autenticación cuando utilice cualquiera de los protocolos definidos en **COM.1**.

52. **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*].

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

53. **ACT.1** El TOE ofrecerá la posibilidad de consultar la versión actual del firmware/software y podrá [**selección**: actualizarse automáticamente; iniciar actualizaciones manualmente] y [**selección**: comprobar si existen nuevas actualizaciones disponibles; ningún otro].
54. **ACT.2** El TOE deberá utilizar [**selección***: hashes publicados; firma digital*] que estén autorizados en la guía CCN-STIC-807 para autenticar las actualizaciones *firmware/software* antes de instalarlas.
55. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.
56. **ACT.4** En el caso de que el TOE sea una *aplicación software*, esta deberá estar empaquetada de forma que, si se elimina, no deje rastro de su instalación (excepto por configuraciones y ficheros de salida o auditoría).
57. **ACT.5** En el caso de que el TOE sea una *aplicación software*, este no descargará ni modificará su propio código binario.

4.6 CRIPTOGRAFÍA

58. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
59. **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.

4.7 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

60. **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**.

4.8 CAPACIDADES ANTI-EXPLOTACIÓN

61. **EXP.3** En el caso de que el TOE sea una aplicación *software*, este solamente utilizará las bibliotecas de terceras partes declaradas [**asignación***: listado de librerías*].

4.9 INFRAESTRUCTURA DE ESCRITORIO VIRTUAL (VDI)

62. **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.

63. **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.

64. **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.

65. **VDI.4.** El TOE 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.).

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

67. **VDI.6.** En caso de que el TOE 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.

4.10 NOTAS DE APLICACIÓN GENERAL

68. 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***.

69. 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*
TOE	*Target of Evaluation*
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