centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC-
Anexo F.13: Conmutadores KVM

Febrero 2023

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
2023.03.01 11:11:16 +01'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2023

NIPO: 083-23-071-5.
Fecha de Edición: Febrero 2023

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Conmutadores KVM** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), publicado por el CCN.

2. Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia debe implementar para un determinado caso de uso, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza y considerarse objetivamente cualificado desde el punto de vista de la seguridad para ser empleado en los sistemas de información del sector público a las que sea de aplicación el Esquema Nacional de Seguridad (ENS). Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.

3. Además, la aplicación de estos criterios permitirá:

   - Que se establezcan unas características mínimas de seguridad que sirvan de referencia a los **fabricantes** a la hora de desarrollar nuevos productos STIC.
   - Que los **organismos responsables de la adquisición** dispongan de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrecen dichos productos.
   - Que los **usuarios finales** posean una guía que facilite el despliegue y garantice el uso apropiado del producto desde el punto de vista de la seguridad.

4. Por lo tanto, los productos catalogados dentro de la familia **Conmutadores KVM** 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 Conmutadores KVM (*Keyboard-Video-Mouse*), son dispositivos de *hardware* que permiten al usuario controlar múltiples ordenadores desde uno o más conjuntos de teclados, monitores de video y ratones. Permiten seleccionar qué ordenador se desea activar, mostrando así su salida de vídeo y siendo controlado por el teclado y ratón.
7. En algunos casos, pueden compartir también otros periféricos, como es el caso de las "tarjetas de acceso común", CAC por sus siglas en inglés (*Common Access Card*).

2.2 CASOS DE USO

8. Dependiendo de las funcionalidades del producto explotadas y de la finalidad o el contexto en que se utilicen, se contemplan tres (3) casos de uso para esta familia de productos tal como se definen a continuación.

2.2.1. CASO DE USO 1 – GESTIÓN Y MONITORIZACIÓN LOCAL

9. En este caso, el usuario controla el dispositivo mediante una interfaz ubicada en el propio dispositivo o un controlador conectado directamente. Los periféricos se conectan mediante cables directamente al dispositivo. Se elige qué ordenador de los conectados activar, el cual será controlado por los periféricos conectados al dispositivo.

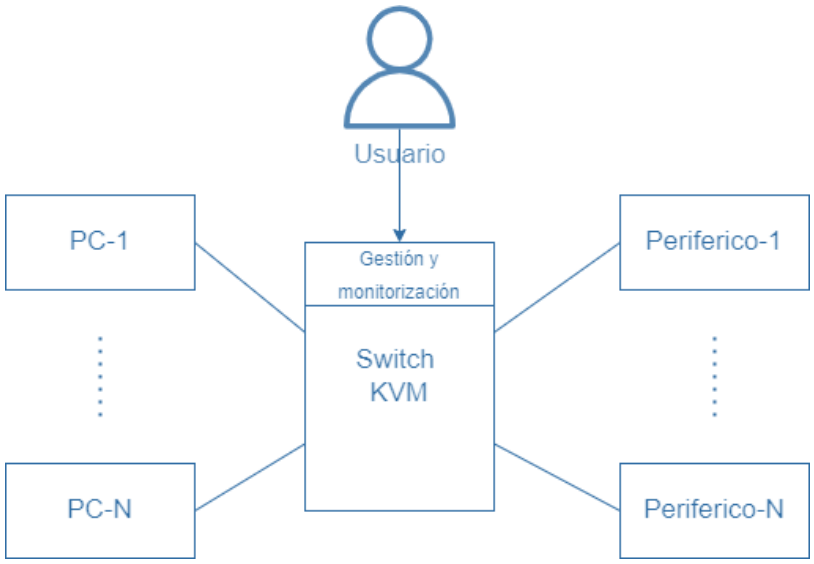

Figura 1 - Caso de uso 1: Gestión y Monitorización local.

2.2.2. CASO DE USO 2 – FILTRO O AISLADOR

10. En este caso, el dispositivo se encuentra conectado a un conjunto de periféricos, pero a un solo ordenador. Dicho ordenador puede cambiar en el tiempo, por ejemplo, distintos ordenadores portátiles que conectan al Aislador que reside en una sala de reuniones o conferencias.

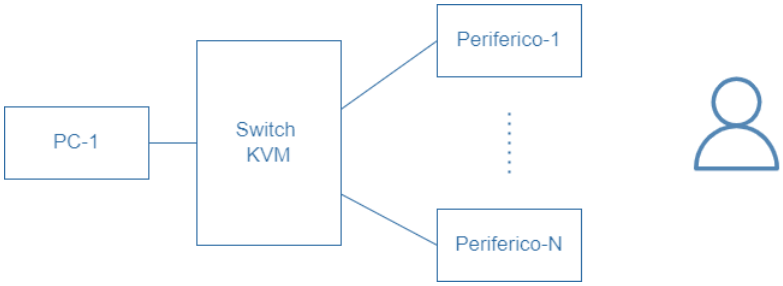

Figura 2 - Caso de uso 2: Filtro o aislador.

2.2.3. CASO DE USO 3 – COMBINADOR

11. En este caso, el dispositivo se emplea para mostrar simultáneamente la salida de vídeo de varios ordenadores conectados a uno o más monitores. Permite combinar la salida de vídeo de varios ordenadores conectados en un único monitor.

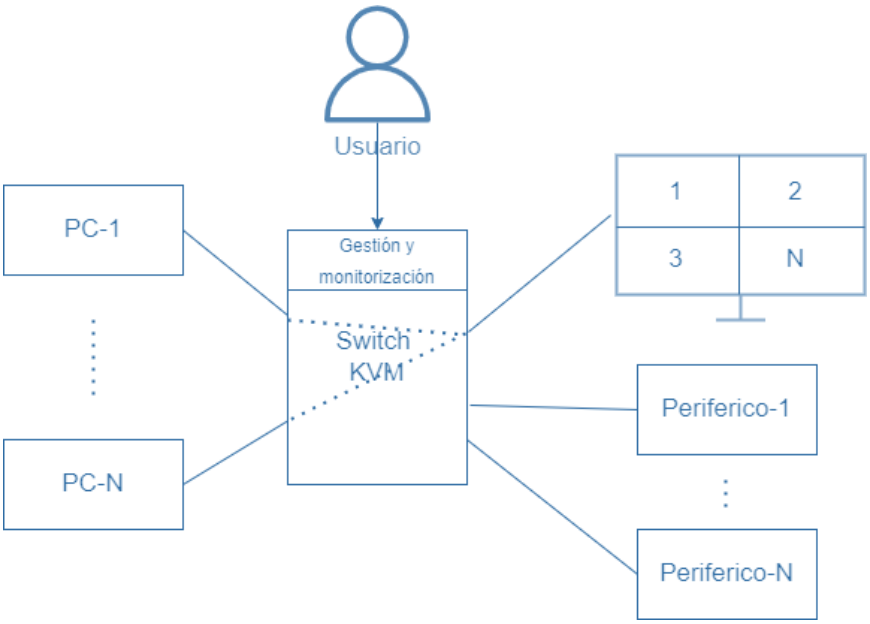

Figura 3 - Caso de uso 3: Combinador.

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

12. Para la utilización en condiciones óptimas de seguridad de los conmutadores KVM, es necesario que se integre en un entorno de trabajo que cumpla una serie de 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.
    - **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.
    - **Funcionalidad limitada.** El producto solo debe proporcionar la funcionalidad de *Conmutadores KVM* 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.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

13. Este tipo de productos suele presentarse en formato de **Equipo dedicado** o (***Appliance***: hardware provisto de firmware dedicado) con las funcionalidades necesarias para cumplir su finalidad y acotadas al servicio específico que presten. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2.1, estas quedan fuera del alcance analizado, debiendo ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

14. 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).

15. En el ámbito de CC se elaboran unos perfiles de seguridad que definen, para un dominio o categoría de productos, un conjunto de objetivos y requisitos de seguridad, tanto funcionales como de evaluación, independientes de la implantación.

16. Los productos dentro de esta familia deberán estar certificados de acuerdo a la norma *Common Criteria*. Dicha certificación deberá evidenciar el problema de seguridad definido en el presente documento e incluir los requisitos fundamentales de seguridad recogidos en el apartado 4.

17. El nivel de confianza EAL (*Evaluation Assurance Level*) con el que deben ser evaluados los requisitos exigidos para esta familia será:

    - **El determinado por el perfil de protección** para aquellos SFR incluidos en los perfiles exigidos cuando los productos se encuentren certificados contra alguno de los perfiles descritos en el apartado 4.1.

18. En caso de que alguno de los requisitos indicados en el apartado 4 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 ACTIVOS SENSIBLES A PROTEGER

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

- **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.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

20. 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.COM1 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.CON Compromiso de credenciales:** Un atacante puede aprovecharse del uso credenciales débiles o desprotegidas, para ganar acceso privilegiado al producto.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

21. A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a la inclusión en el CPSTIC en esta familia.

4.1 PERFIL DE PROTECCIÓN

22. **REQ.1** Los productos deberán estar certificados con el siguiente perfil de protección y los siguientes módulos certificados de acuerdo a la norma *Common Criteria*:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Peripheral Sharing Device[1]	4.0	19/07/2019	NIAP
Módulo	**Versión**	**Fecha**	**Organismo responsable**
PP-Module for Analog Audio Output Devices[2]	1.0	19/07/2019	NIAP
PP-Module for Keyboard/Mouse Devices[3]	1.0	19/07/2019	NIAP
PP-Module for Video/Display Devices[4]	1.0	19/07/2019	NIAP

23. **REQ.2** En caso de que el producto permita la integración con tarjetas de acceso común (CAC - *Common Access Card*), deberá estar certificado también con el siguiente módulo de acuerdo a la norma *Common Criteria:*

PERFIL DE PROTECCIÓN			
Módulo	**Versión**	**Fecha**	**Organismo responsable**
PP-Module for User Authentication Devices[5]	1.0	19/07/2019	NIAP

[1] https://www.niap-ccevs.org/MMO/PP/pp_psd_v4.0.pdf
[2] https://www.niap-ccevs.org/MMO/PP/mod_ao_v1.0.pdf
[3] https://www.niap-ccevs.org/MMO/PP/mod_km_v1.0.pdf
[4] https://www.niap-ccevs.org/MMO/PP/mod_vi_v1.0.pdf
[5] https://www.niap-ccevs.org/MMO/PP/mod_ua_v1.0.pdf

4.2 REQUISITOS CRIPTOGRÁFICOS

24. **REQ. 3** Todos los algoritmos de cifrado simétrico, asimétrico, protocolos de acuerdo de clave y funciones resumen que utilice el producto deberán encontrarse dentro de los acreditados por el CCN para su uso en el ENS. El listado de dichos algoritmos se encuentra recogido en la CCN-STIC-807 Criptología de empleo en el ENS (Categoría ALTA).

5. ABREVIATURAS

ACL	*Access Control List*
CAC	*Common Access Card*
CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
EAL	*Evaluation Assurance Level*
ENS	*Esquema Nacional de Seguridad*
HTTPS	*Hypertext Transfer Protocol Secure*
IPSEC	*Internet Protocol Security*
KVM	*Keyboard-Video-Mouse*
NAS	*Network Attached Storage*
RFS	Requisitos Fundamentales de Seguridad
RMS	*Rights Management System*
SAS	*Serial Attached SCSI (Small Computer System Interface)*
TLS	*Transport Layer Security*

PUBLICACIONES DE DEFENSA

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