GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC - Anexo B.3: Herramientas de gestión de red

Noviembre 2017

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

NIPO: 785-17-037-2.

Fecha de Edición: noviembre 2017
ISDEFE ha participado en el desarrollo del presente documento.

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Herramientas de Gestión de Red** 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 **Herramientas de Gestión de Red** 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 esta familia están orientados fundamentalmente a centralizar, gestionar y configurar la infraestructura de dispositivos que conforman una red, monitorizar su rendimiento y consumo de recursos, y resolver problemas en la red. Engloban todos aquellos aspectos que es necesario considerar a la hora de implementar la infraestructura de comunicaciones de la entidad, con el objeto de asegurar la privacidad y la integridad de la información, así como mantener en servicio el acceso a los recursos corporativos y un tráfico de datos fluido.

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

   - **Monitorización y gestión de la red.** Permite recibir y configurar parámetros de red de los diferentes dispositivos incluyendo parámetros de rendimiento y seguridad.
   - **Definición de plantillas de configuración y capacidades.** Permite aplicar de manera automática una configuración establecida de seguridad y uso de capacidades para los distintos servicios o dispositivos de red.
   - **Generación de informes del uso y rendimiento de la red**. Permite tener un registro del tráfico de la red a partir de los registros de la auditoria de seguridad definidos.
   - **Mecanismos de alerta, gestión de eventos y respuesta automatizada.** Permite detectar en poco tiempo un cambio en las condiciones de funcionamiento de cualquier elemento de la infraestructura y ofrecer la información necesaria para corregir su impacto.

2.2 CASOS DE USO

8. Para esta familia de productos se contemplan dos casos de uso, en función de que la gestión de la red requiera o no de agentes desplegados en los sistemas involucrados. Las políticas de seguridad con las que se configura el producto pueden variar en cada caso, e incluir más o menos restricciones.

2.2.1. CASO DE USO 1 – GESTIÓN DE RED CENTRALIZADA

9. El producto está conectado a una red y tiene un rol de **gestión de la infraestructura**. Se encarga de monitorizar y configurar adecuadamente cada uno de los distintos equipos de la red, haciendo uso de interfaces y protocolos

estándar de red al efecto (p.ej. SNMP[1], ICMP[2], MCTP[3], IPMI[4], etc.), a partir de la definición de la misma y de los elementos que la componen.

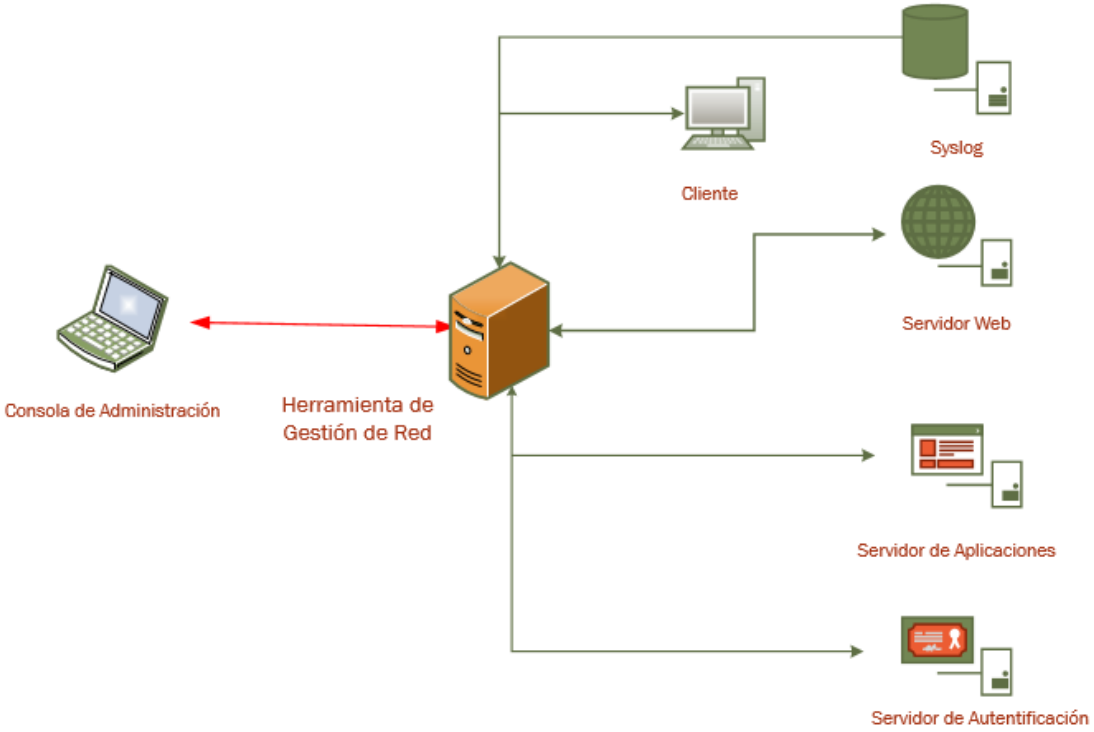

Figura 1.Ejemplo de Caso de Uso 1: Gestión de Red Centralizada.

2.2.2. CASO DE USO 2 – GESTIÓN DE RED DISTRIBUIDA (AGENTES)

10. El producto tiene la misma funcionalidad que en el caso anterior, pero en este caso cuenta con agentes desplegados en los distintos elementos de la red actuando como interfaz *ad hoc* con la herramienta para proporcionarle información sobre los parámetros relevantes del elemento en que se despliegan, así como para implementar localmente los cambios de configuración necesarios.
11. Las comunicaciones entre la herramienta centralizada y los agentes distribuidos podrían implementarse mediante protocolos propietarios o mediante las interfaces y los protocolos estandarizados mencionados en el caso de uso anterior.

[1]*Simple Network Management Protocol*. Protocolo simple de administración de Red
[2]*Internet Control Message Protocol*. Protocolo de control de mensajes de Internet
[3]*Management Component Transport Protocol*
[4]*Intelligent Plattform Management Interface*

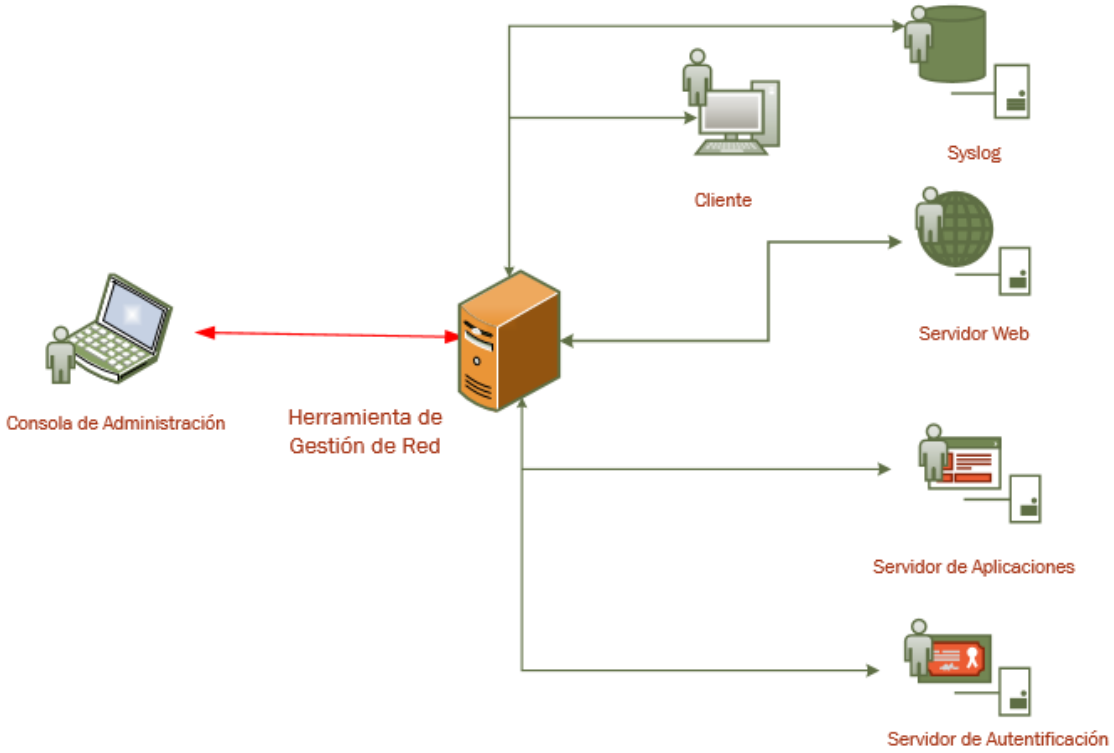

Figura 2.Ejemplo de Caso de Uso 2: Gestión de Red Distribuida (Agentes)

2.3 ENTORNO DE USO

12. Por lo general, este tipo de dispositivos se encuentran en grandes o medianas empresas, así como en redes del sector público, como parte de una arquitectura de defensa en profundidad, en combinación con medidas complementarias en diferentes capas de protección.
13. Para que trabajen en condiciones óptimas de seguridad, es necesario que se integren en un entorno operacional que cumpla las siguientes condiciones mínimas de protección:

- **Protección física.** El producto deberá instalarse en un área donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas. En el caso de que se trate de una herramienta de gestión distribuida este requisito no aplicará a los distintos agentes.
- **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 dañina al administrar el producto.
- **Funcionalidad limitada**: El producto deberá utilizarse para la conmutación de redes como su función básica y no proporcionar ninguna otra funcionalidad, salvo aquellas determinadas compatibles orientadas a la protección de las comunicaciones.

- **Actualizaciones periódicas**. El producto será puesto al día conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **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

14. Este tipo de productos se presentan en formato **Software** o de **equipo dedicado** (***appliance*)** (hardware provisto de firmware dedicado) con las funcionalidades estrictamente necesarias para cumplir su finalidad y acotadas al servicio específico que presten.
15. Adicionalmente, suele ser habitual que en las máquinas y dispositivos con los que interactúa dentro de la red se incluya un componente **Software** instalable (agente)que ejerce un papel de interfaz para la recopilación de información y el control de las entidades conectadas en la red.
16. Por último, para realizar las funciones de control y administración del dispositivo es normal incluir con el producto un **Software** específico para instalarlo en un equipo informático estándar.
17. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 4, éstas quedan fuera del alcance analizado y deberán ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

18. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TI (Tecnologías de la Información).
19. 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.
20. Los productos dentro de esta familia deberán estar certificados con uno de los siguientes perfiles de protección certificados de acuerdo a la norma *Common Criteria,* junto con los restantes requisitos fundamentales de seguridad recogidos en la sección 4:

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Collaborative Protection Profile for Network Devices.[5]	1.0	27/02/2015	CCDB[6]
Protection Profile for Network Devices.[7]	1.1	08/06/2012	NIAP[8]

Tabla 1. Perfiles de protección

21. 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 anteriormente descritos.
    - **EAL2 o superior** para los RFS adicionales que no encuentren incluidos dentro de un perfil.
    - **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra ningún perfil.

[5] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf
[6] *Common Criteria Development Board*
[7] https://www.commoncriteriaportal.org/files/ppfiles/PP_ND_V1.1.pdf
[8] *National Information Assurance Partnership*

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

22. Los recursos que es necesario proteger mediante el uso de estos productos incluyen:

    - Credenciales de los usuarios y los servicios a los que es posible acceder desde la red corporativa.
    - Información sensible que pueda almacenar el producto en su configuración o en el dispositivo hardware donde haya sido desplegado.
    - Información sensible que pueda recibirse a través de los ficheros de registro de eventos de los equipos y servicios para su tratamiento en el producto.
    - Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos.
    - Datos de configuración del producto y de auditoría generados por éste.
    - Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

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

    - **Escucha de red.** Un atacante se coloca en una conexión inalámbrica o en otro lugar de la infraestructura de red. El atacante puede supervisar y obtener el acceso a la comunicación y/o los datos intercambiados entre el producto y otros puntos finales de la red.
    - **Divulgación de la información no autorizada.** Un atacante consigue recopilar información no autorizada del dispositivo (p. ej., servicios de la organización, credenciales, etc.).
    - **Suplantación de la identidad de usuarios registrados.** El atacante suplanta la identidad de usuarios legítimos mediante la apropiación de credenciales o medios de entrada ajenos, pudiendo obtener acceso al producto o a los servicios que estaban reservados a dichos usuarios. Este tipo de ataques activos pueden utilizar técnicas de ataque tales como la explotación de contraseñas, secuestro de sesión, ataques hombre en el medio, etc.
    - **Denegación de servicio.** Un agente deniega el servicio de identificación utilizando técnicas y ataques de denegación de servicios remotos, imposibilitando el acceso al entorno operacional por parte de los usuarios.
    - **Uso de canales de comunicación inseguros.** Permiten a un atacante comprometer la integridad y la confidencialidad de las comunicaciones del

producto. El atacante puede tener acceso a la red o a partes de la red que contienen tráfico acerca de las políticas del servidor, manejo de fuentes y repositorios de políticas de seguridad.

- **Compromiso de la funcionalidad del dispositivo.** Un atacante o un fallo en el dispositivo compromete la funcionalidad de seguridad, permitiendo modificarla o desactivarla de manera no conforme a las políticas de seguridad (p.ej., instalación de actualizaciones maliciosas o administración no autorizada del dispositivo).
- **Cifrado débil.** Utilización en el dispositivo de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente, mediante ataques de fuerza bruta.
- **Acceso no autorizado.** Un atacante consigue acceder a información, intercambiada a través del producto, así como generada o almacenada en él, para la que no estaba autorizado (p.ej., información almacenada en memoria).

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

24. 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

25. **REQ. 1** Los productos deberán estar certificados con uno de los siguientes perfiles de protección certificados de acuerdo a la norma *Common Criteria:*

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Collaborative Protection Profile for Network Devices.[9]	1.0	27/02/2015	CCDB
Protection Profile for Network Devices.[10]	1.1	08/06/2012	NIAP

Tabla 2. Perfiles de protección

26. **REQ. 2** En caso de que el producto no esté certificado contra ninguno de los perfiles anteriores, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) de *Collaborative Protection Profile for Network Devices V.1.0* con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.2 REQUISITOS CRIPTOGRÁFICOS

27. **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).

4.3 CONFIGURACIÓN DEL PRODUCTO

28. **REQ. 4** El producto permitirá el alta, baja o modificación de los dispositivos a gestionar, asociando los parámetros básicos para su identificación de forma inequívoca y para el establecimiento de las comunicaciones de red seguras.

29. **REQ. 5** El producto permitirá seleccionar la frecuencia de refresco de consulta automática, para los parámetros básicos relacionados con la disponibilidad y

[9] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf
[10] https://www.commoncriteriaportal.org/files/ppfiles/PP_ND_V1.1.pdf

rendimiento de los dispositivos, u otros parámetros de interés para la seguridad gestionados.

30. **REQ. 6** El producto permitirá realizar consultas que permitan al usuario seleccionar los parámetros de interés gestionados, para uno o varios sistemas.
31. **REQ. 7** El producto debe mostrar avisos a los usuarios asociados al incumplimiento de condiciones previamente definidas.
32. **REQ. 8** El producto debe registrar todos los avisos que se han producido.
33. **REQ. 9** El producto debe solicitar confirmación a un usuario autorizado antes de la ejecución de acciones que supongan cambios en la configuración de seguridad de los dispositivos/agentes distribuidos.

4.4 PRIVILEGIOS

34. **REQ. 10** El producto deberá de disponer de los siguientes roles de usuario:
    a. Rol con acceso a las funciones de monitorización en la herramienta de gestión.
    b. Rol con acceso a las funciones de configuración de los sistemas/agentes remotos.
    c. Rol con acceso a las funciones de administración de la herramienta de gestión.

5. ABREVIATURAS

CC	*Common Criteria*
CCDB	*Common Criteria Development Board*
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*
ICMP	*Internet Control Message Protocol*
IPMI	*Intelligent Plattform Management Interface*
MCTP	*Management Component Transport protocol*
NIAP	*National Information Assurance Partnership*
PYTEC	*Productos y tecnologías*
RFS	*Requisitos Fundamentales de Seguridad*
SFR	*Security Functional Requirements*
SNMP	*Simple Network Management Protocol*