centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo B.3-M: Herramientas de gestión de red

Diciembre 2019

MINISTERIO DE DEFENSA

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.12.27 13:12:42 +01'00'

NIPO: 083-19-053-9.

Fecha de Edición: diciembre 2019

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 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 **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.

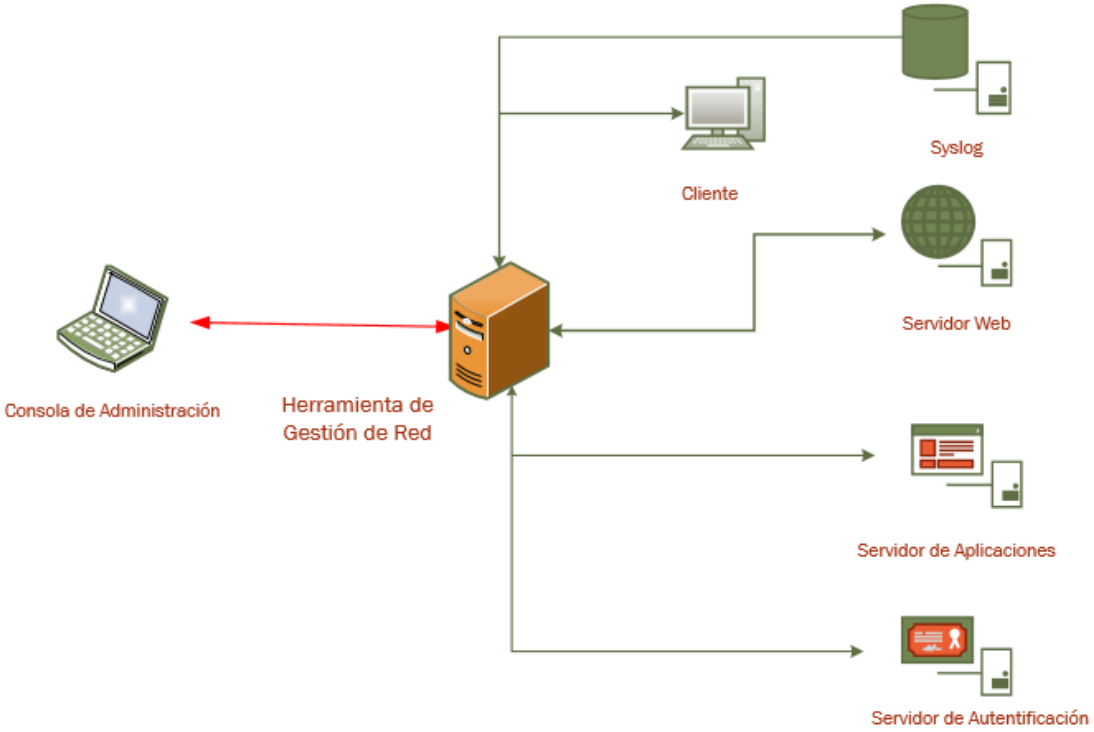

Figura 1. Ejemplo de Caso de Uso 1: Gestión de Red Centralizada.

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*

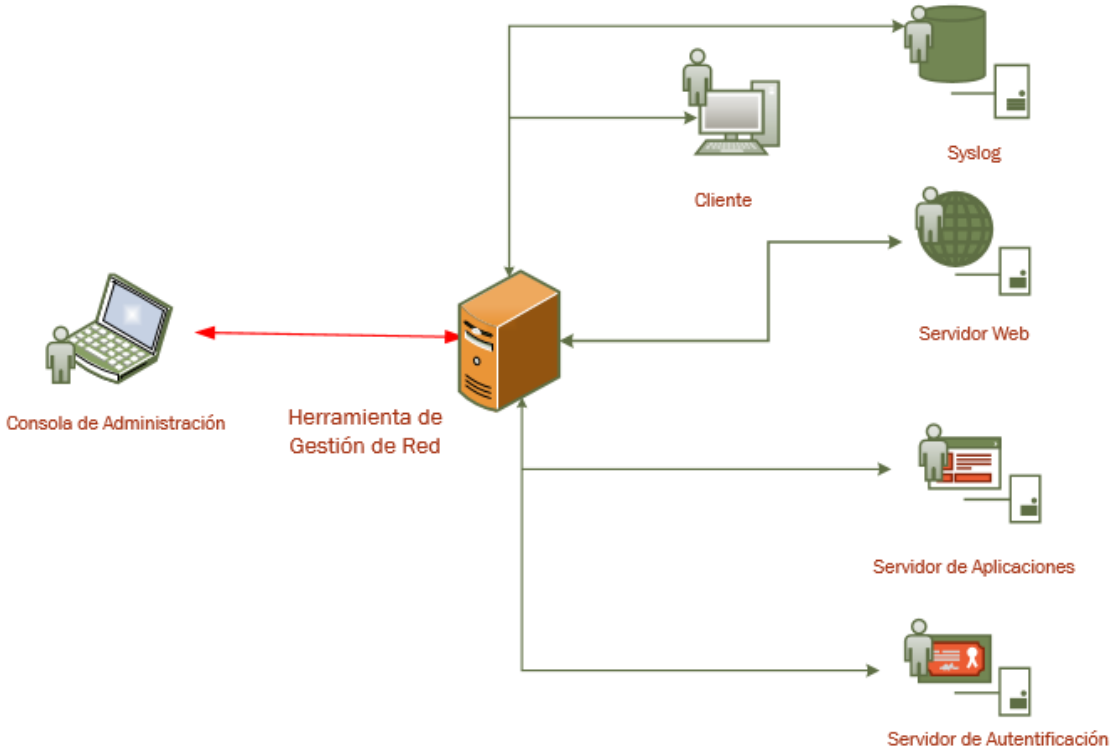

Figura 2. Ejemplo de Caso de Uso 2: Gestión de Red Distribuida (Agentes)

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 CERTIFICACIÓN LINCE

18. 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)[5] que incluya los RFS reflejados en el apartado 4, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.
19. 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) de Evaluación Criptográfica (MEC) serán opcionales.

[5] 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 RECURSOS QUE ES NECESARIO PROTEGER

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

    - AC Administración. Interfaces de gestión del producto e información transmitida a través de ellas, en ambos sentidos.
    - AC Datos. Datos de configuración del producto y de auditoría generados por éste. Información que atraviese el producto entre sus interfaces de red. Credenciales de usuario.
    - AC. Actualizaciones. Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

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

    - **A.CIFRA Cifrado débil:** Utilización en el dispositivo de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
    - **A.RED Ataque a la red.** Un atacante, desde dentro o desde fuera de la red, consigue acceder a información intercambiada a través de la red entre el producto y otras entidades autorizadas o modificar sus comunicaciones.
    - **A.ACT Actualización maliciosa:** un atacante puede realizar una actualización maliciosa que debilite las funcionalidades de seguridad del producto.
    - **A.NODET Actividades no detectadas:** Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador.
    - **A.CRED Compromiso de credenciales:** un atacante puede comprometer las credenciales o información del producto permitiendo un acceso continuado al producto y a su información sensible.
    - **A.NOAUT Acceso no autorizado de administrador:** Un atacante puede obtener un acceso cómo administrador del producto haciéndose pasar por un administrador ante el producto, por el producto ante un administrador, reproduciendo una sesión de administración, realizando ataques del hombre en medio.
    - **A.FUN Fallo de las funcionalidades de seguridad**: Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad del producto y podría acceder, cambiar o modificar información o funcionalidades de seguridad del producto.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

22. 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 AUDITORÍA

23. Estas funcionalidades de seguridad mitigan la amenaza (A.NODET).
24. **AUD.1.** El producto debe generar información 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 usuarios registrados.
    b) Cambios en la configuración del producto.
    c) Generación, importación, cambio o eliminación de claves criptográficas.
    d) Cambios en las credenciales de usuarios.
    e) Otros eventos de seguridad relevantes (definir).
25. **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).
26. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:
    a) Lectura: Sólo usuarios autorizados.
    b) Modificación: Ningún usuario.
    c) Borrado: solo Administradores.
27. **AUD.4.** El producto debe ser capaz de almacenar la información de auditoría generada en sí mismo o en una entidad externa.
28. **AUD.5.** El producto debe ser capaz de eliminar o sobrescribir registros de auditoría anteriores cuando el espacio de almacenamiento esté lleno.

4.2 ADMINISTACIÓN

29. Estas funcionalidades de seguridad mitigan la amenaza (A.NOAUT).
30. **ADM.1** El producto debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.
31. **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 (definir).

32. **ADM.3.** El producto deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones anteriormente descritas.

4.3 IDENTIFICACIÓN Y AUTENTICACIÓN

33. Estas funcionalidades de seguridad mitigan la amenaza (A.CRED y A.NOAUT).

1. **IAU.1** El producto deberá identificar y autenticar a cada usuario antes de otorgar acceso a la funcionalidad del producto. Deberá especificarse qué acciones puede llevar a cabo un usuario antes de ser identificado y autenticado.
2. **IAU.2** El producto deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
3. **IAU.3.** El producto deberá proteger de lectura y modificación no autorizada las credenciales de autenticación.
4. **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 [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “]

4.4 CRIPTOGRAFÍA

5. Estas funcionalidades de seguridad mitigan la amenaza (A.CIFRA).
6. **CIF.1** El TOE permitirá exclusivamente el empleo de funciones, algoritmos y protocolos que utilicen suites de cifrado que estén incluidas entre las autorizadas para Categoría Media del ENS, de acuerdo a lo establecido en la guía CCN-STIC-807.
7. **CIF.2** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLE

8. Estas funcionalidades de seguridad mitigan la amenaza (A.ACT).
9. **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.

10. **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.
11. **ACT.3** La actualización del firmware/software se permitirá únicamente a usuarios con rol de administrador.

4.6 CANALES DE COMUNICACIÓN CONFIABLES

12. Estas funcionalidades de seguridad mitigan la amenaza (A.RED).
13. **COM.1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas (auditoría, administración, etc.) 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.).
14. **COM.2** El TOE debe permitir que estos canales de comunicación seguros sean iniciados por él mismo o por entidades autorizadas.

4.7 CONFIGURACIÓN DEL PRODUCTO

15. Estas funcionalidades de seguridad mitigan la amenaza (A.FUN).
16. **GES.1:** El producto permitirá el alta, baja o modificación de los dispositivos que gestiona, y asociará los parámetros básicos para su identificación de forma inequívoca y para el establecimiento de las comunicaciones de red seguras.
17. **GES.2** El producto deberá mostrar a los usuarios avisos asociados al incumplimiento de condiciones previamente definidas.
18. **GES.3 El** producto deberá registrar todos los avisos que se han producido.
19. **GES.4** 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.

4.8 PRIVILEGIOS

20. Estas funcionalidades de seguridad mitigan la amenaza (A.FUN).
21. **PRI.1** 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

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*