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.6: Sistemas de gestión de eventos de seguridad

Noviembre 2017

Edita:

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

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2017.11.27 11:17:54 +01'00'

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 **Sistemas de Gestión de Eventos de Seguridad** 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 **Sistemas de Gestión de Eventos de Seguridad** 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 a recopilar información en tiempo real sobre los eventos de seguridad generados por la red de una organización, para procesarla posteriormente con el fin de generar informes y/o alertas que puedan ayudar a la organización en la toma de decisiones en materia de seguridad.
7. Son productos que se conciben como una plataforma de gestión de la seguridad lógica de la red sobre la que se implantan y se enfocan principalmente en los siguientes aspectos:
   - Gestión centralizada de los registros y eventos de seguridad generados por los sistemas.
   - Análisis o monitorización en tiempo real de los eventos de seguridad de múltiples fuentes.
   - Utilización de sistemas de gestión de bases de datos para consolidar la información.
8. Estos productos suelen estar desarrollados por módulos, cada uno de ellos con funciones específicas. Además, pueden contar con agentes recopiladores de registros, servidores de almacenamiento con bases de datos, motores de correlación de datos para ofrecer información relevante, etc.
9. En este contexto las funciones básicas de seguridad que proporcionan esta familia de productos son las siguientes:
   - **Gestión de múltiples fuentes de datos.** Permiten administrar ficheros de registros de eventos provenientes de diversas fuentes como servidores, bases de datos, aplicaciones, etc, así como consolidar dichos datos y preservar su integridad ante modificaciones no autorizadas.
   - **Correlación**. Cuentan con la capacidad de buscar atributos comunes y/o las relaciones entre los ficheros de registro de eventos de todas las fuentes. Estos productos ofrecen una variedad de técnicas de correlación para integrar diferentes fuentes de datos con el fin de convertir los datos brutos en información de calidad para la organización.
   - **Servicios de alertas**. A partir del análisis automatizado de eventos correlacionados, estos productos son capaces de permitir la programación de alertas para notificar a los destinatarios problemas o incidencias de manera inmediata. Una alerta puede ser enviada a una consola o pantalla, o a través de canales de terceros como el correo electrónico.
   - **Repositorio de datos sobre eventos de seguridad.** Estas soluciones pueden guardar la información registrada sobre eventos de seguridad de los

sistemas que se integran con ella, y servir de gran ayuda a la investigación forense de incidentes de seguridad.

2.2 CASOS DE USO

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

2.2.1. CASO DE USO 1- REPOSITORIO CENTRALIZADO DE EVENTOS DE SEGURIDAD

11. El producto se sitúa en un punto de la arquitectura de red de la organización donde pueda maximizar la recepción de información relativa a registros y eventos de todos los servicios y equipos de una red. Una vez conseguidos todos los datos, éstos son procesados y almacenados para asegurar su integridad.

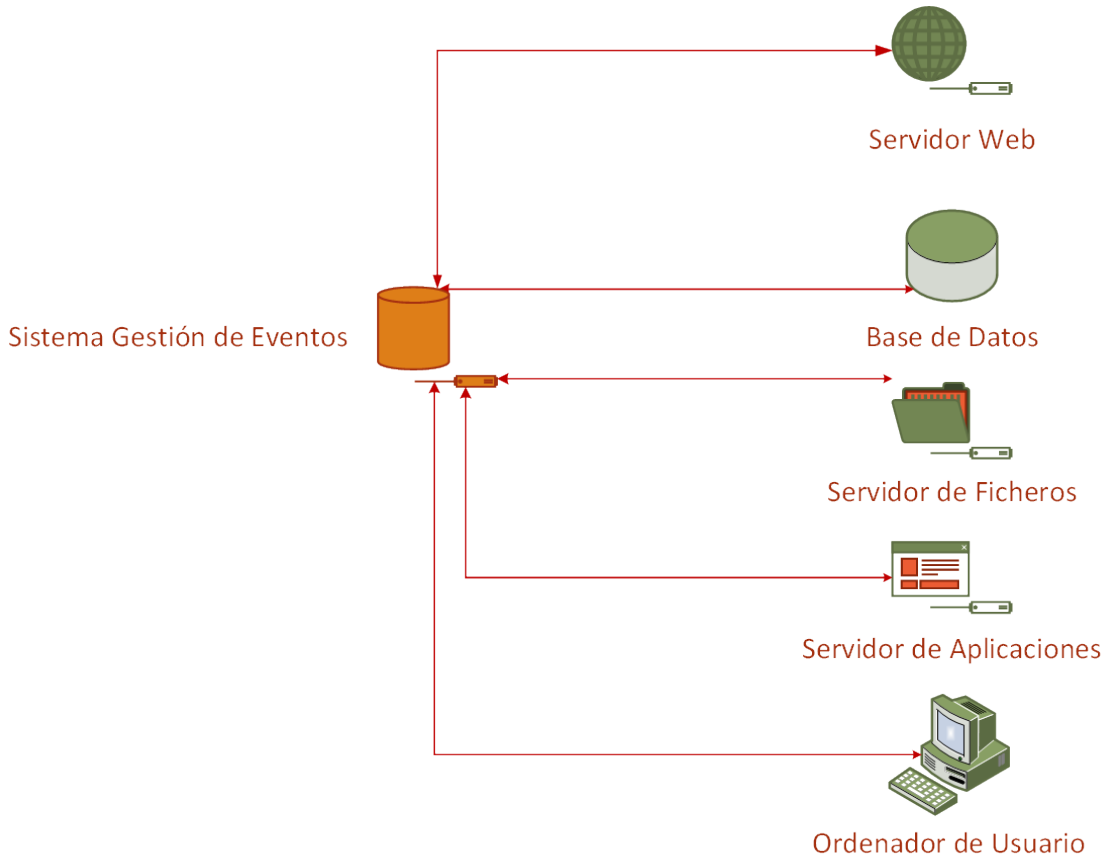

Figura 1. Ejemplo de Caso de Uso 1: Repositorio Centralizado de Eventos de Seguridad

12. En este caso, el producto actúa únicamente como un repositorio de información, ya que no realiza ningún procesamiento posterior.

2.2.2. CASO DE USO 2 - REPOSITORIO CENTRALIZADO Y CORRELACIÓN DE EVENTOS

13. Este es el caso de uso más habitual de este tipo de productos. Al igual que en el caso anterior, el producto se sitúa de forma que pueda recopilar registros y eventos de todos los servicios y equipos de una red. Posteriormente, el producto trata esta información para generar informes y alertas que han sido previamente definidas.

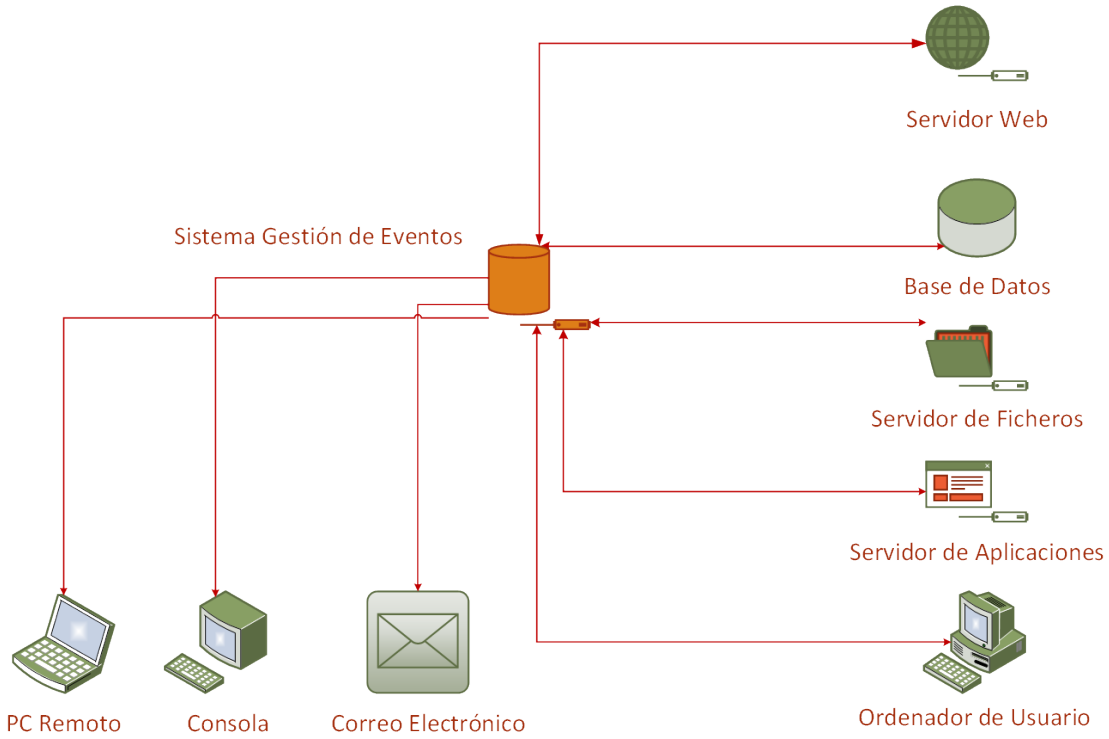

Figura 2. Ejemplo de Caso de Uso 2: Repositorio Centralizado y Correlación de Eventos

2.3 ENTORNO DE USO

14. Por lo general, estas herramientas se encuentran en grandes o medianas empresas, así como en redes del sector público, formando parte de una arquitectura de defensa en profundidad que busca asegurar la existencia de registros de auditoría de seguridad para detectar o poder analizar posibles incidentes de seguridad.

15. Para la utilización en condiciones óptimas de seguridad, es necesaria su integración 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.

- **Plataforma segura**: El producto se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.
- **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.
- **Actualizaciones periódicas:** El software del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **Política de seguridad de la Información.** La política de seguridad deberá recoger el conjunto de principios, la organización y los procedimientos impuestos por una organización para hacer frente a sus necesidades de seguridad de la información, incluyendo el uso de las TIC.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

16. Este tipo de productos se puede presentar en formato de **equipo dedicado** (***Appliance***: hardware provisto de firmware[1]y software dedicado) o en forma de aplicación **Software** con las funcionalidades estrictamente necesarias para cumplir su finalidad y acotadas al servicio específico que presten.
17. Adicionalmente, 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.
18. En caso de ofrecer funcionalidades adicionales a las definidas en la sección **¡Error! No se encuentra el origen de la referencia.**, éstas 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)

19. 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).
20. 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.
21. Los productos dentro de esta familia deberán cumplir con los SFR (*Security Functional Requirements*) que se especifican en uno de los siguientes perfiles de

[1]*Firmware* funciona como el nexo de unión entre las instrucciones (*software*) que llegan al dispositivo desde el exterior y las diversas partes electrónicas (*hardware*).

protección certificado de acuerdo a la norma *Common Criteria,* junto con los restantes requisitos fundamentales de seguridad recogidos en la sección 4:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Application Software.	1.2	25/04/2016	NIAP
Collaborative Protection Profile for Network Devices.[2]	1.0	27/02/2015	CCDB
Protection Profile for Network Devices.[3]	1.1	08/06/2012	NIAP

Tabla 1. Perfil de protección

22. 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.

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

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:

- Información sensible que pueda recibirse sobre los registros de eventos de seguridad de los equipos y servicios para su tratamiento en el producto.
- Información generada por el producto tras el procesamiento y correlación de los eventos de seguridad.
- 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

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

- **Divulgación de información no autorizada:** Un atacante consigue recopilar información no autorizada del producto (p.ej. servicios de la organización, credenciales, etc.).
- **Escucha de red:** Un atacante, desde dentro o desde fuera de la red, consigue acceder a información intercambiada entre los distintos módulos de la aplicación.
- **Acceso no autorizado**: Un atacante consigue acceso no autorizado a información intercambiada a través del producto, o que ha sido generada o almacenada en él (p.ej.: información almacenada en memoria).
- **Acciones no autorizadas.** Un usuario podría obtener acceso no autorizado a los recursos. Un usuario, proceso o entidad externa malicioso, se podría enmascarar como una entidad autorizada, para obtener un acceso no autorizado a los recursos del producto.
- **Cifrado débil**: Utilización en el producto de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
- **Uso de canales de comunicación inseguros**: Mala implementación de protocolos estándar o utilización de protocolos no estandarizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones del producto.

- **Compromiso de la funcionalidad del producto**: Un atacante o un fallo en la herramienta 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 de la herramienta).

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.

4.1 REQUISITOS CRIPTOGRÁFICOS

26. **REQ. 1** 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 (Categoría ALTA).

4.2 PRODUCTO *APPLIANCE*

27. **REQ. 2** En caso de que el producto sea un equipo dedicado o *Appliance,* deberá estar certificado con uno de los siguientes perfiles de protección publicados certificados de acuerdo a la norma *Common Criteria:*

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Collaborative Protection Profile for Network Devices.[4]	1.0	27/02/2015	CCDB
Protection Profile for Network Devices.[5]	1.1	08/06/2012	NIAP

Tabla 2. Perfiles de protección

28. **REQ. 3** En caso de que el producto no esté certificado contra ningún perfil de los anteriores, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) del perfil *Collaborative Protection Profile for Network Devices. Version 1.0.*con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.3 PRODUCTO SOFTWARE

29. **REQ. 4** En caso de que el producto sea únicamente Software ,deberá estar certificado con uno de los siguientes perfiles de protección publicados certificados de acuerdo a la norma *Common Criteria:*

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

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Application Software.[6]	1.2	25/04/2016	NIAP

Tabla 3. Perfil de protección

30. **REQ. 5** En caso de que el producto no esté certificado contra el perfil indicado, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) de éste con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.4 REGISTRO DE EVENTOS

31. **REQ. 6** El producto debe ser capaz de recibir, identificar o interpretar eventos basados en diferentes fuentes de registros de eventos (p.ej.: Syslog) y objetos serializados para el tratamiento de incidentes y recomendaciones.
32. **REQ. 7** Cuando el producto tenga funcionalidades para la correlación de eventos de seguridad, facilitará la creación de alarmas en caso de detectar potenciales riesgos para la seguridad.

4.5 REGISTROS AUDITORIA

33. **REQ. 8** Se debe proporcionar un medio para almacenar los eventos relacionados con la seguridad, de forma que permita interpretarse por un usuario.
34. **REQ. 9** 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.
35. **REQ. 10** Se registrarán en la auditoria los siguientes eventos:
    a. Iniciar o detener la auditoria de la aplicación.
    b. Cambios en el grupo de usuario que tiene el rol de administrador.
    c. Utilización por parte del usuario de los mecanismos de autenticación.
    d. Cualquier utilización de los mecanismos de autenticación del producto.
    e. Cambios de la configuración del producto.
36. **REQ. 11** Los registros de auditoría solo podrán ser modificados por usuarios autorizados.
37. **REQ. 12** Sólo podrán leer los registros de auditoría los usuarios autorizados.

[6] https://www.commoncriteriaportal.org/files/ppfiles/pp_app_v1.2.pdf

38. **REQ. 13** Los administradores serán los únicos usuarios que puedan borrar registros de auditoría.

4.6 IDENTIFICACIÓN Y AUTENTICACIÓN

39. **REQ. 14** El producto debe mantener una lista de atributos de seguridad perteneciente a cada usuario. Los atributos serán, al menos, los siguientes:
    a. Identificación única de usuario.
    b. Contraseña / método de acceso.
    c. Rol de usuario y su estado actual (habilitado o no).
40. **REQ. 15** El producto requerirá que cada usuario sea autenticado correctamente antes de permitir cualquier otra acción en el producto en nombre de ese usuario.

5. ABREVIATURAS

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*
NIAP	*National Information Assurance Partnership*
RFS	*Requisitos Fundamentales de Seguridad*
SFR	*Security Functional Requirements*
SYSLOG	*Estándar de mensajes de registro*