centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC –
Anexo B.6-M: Sistemas de gestión de eventos de seguridad

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
2020.02.13 17:37:42 +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 **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) 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 **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

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.

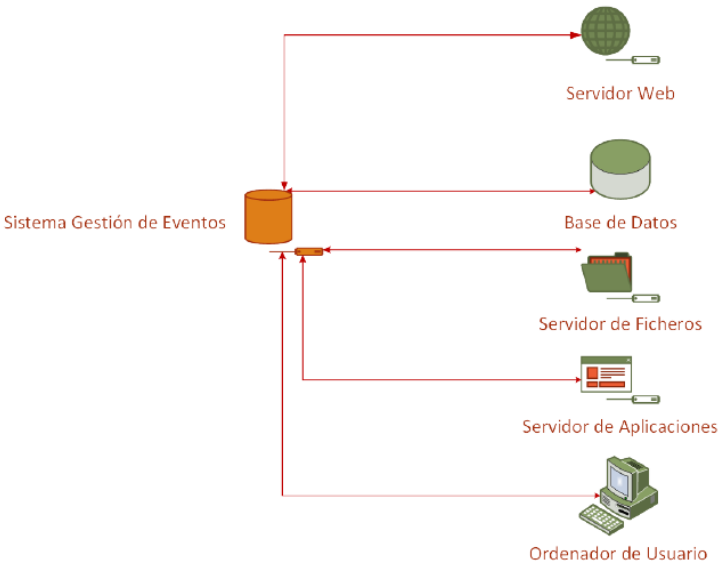

Figura 1. Ejemplo de Caso de Uso 1: Repositorio centralizado de eventos de seguridad.

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

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.

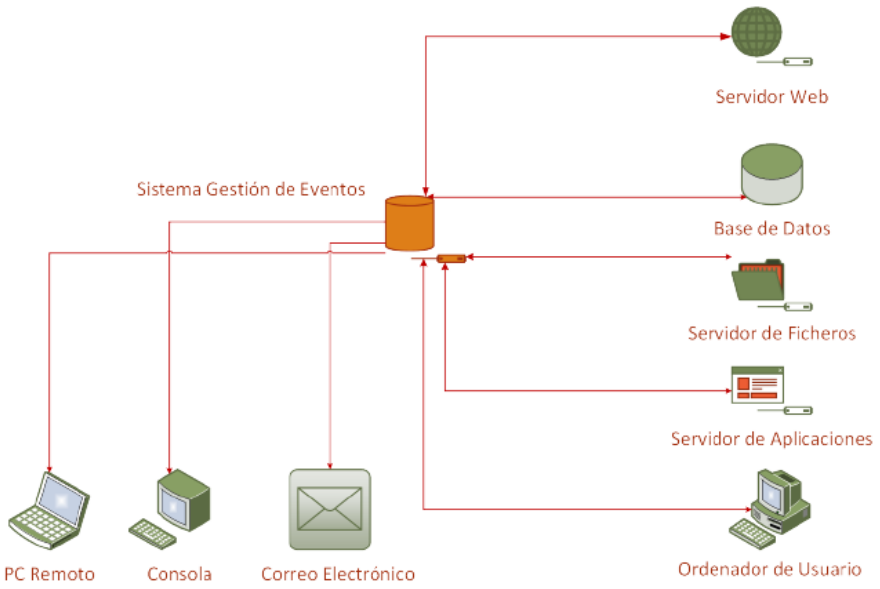

Figura 2. Ejemplo de Caso de Uso 2: Repositorio centralizado y correlación de eventos.

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:

    a) **Protección física:** El producto deberá instalarse en un área donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.

    b) **Plataforma segura:** El producto se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.

    c) **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.

    d) **Actualizaciones periódicas**: El software del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.

    e) **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 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 2.1, éstas quedan fuera del alcance analizado, debiendo ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 CERTIFICACIÓN LINCE

19. Para que un producto de esta familia pueda ser incluido en el CPSTIC bajo la categorización de ENS 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.

[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 RECURSOS QUE ES NECESARIO PROTEGER

20. Los recursos a proteger mediante el uso de estos 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

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

    a) **Divulgación de información no autorizada:** Un atacante consigue recopilar información no autorizada del producto (p.ej. servicios de la organización, credenciales, etc.).

    b) **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.

    c) **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).

    d) **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.

    e) **Cifrado débil**: Utilización en el producto de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.

    f) **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.

    g) **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)

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. **REQ. 1** El producto deberá generar registros de auditoría al comienzo y finalización de las funciones de auditoría y cuando se produzca, al menos, alguno de los siguientes eventos:

    a) *Login* y *logout* de personal autorizado. (En caso de que la funcionalidad de autenticación no esté cubierta por el entorno).

    b) Cambio en las credenciales de usuarios. (En caso de que implemente gestión de credenciales).

    c) Cambios en la configuración del producto.

    d) Eventos relativos a la funcionalidad de SIEM.

24. **REQ. 2** Para cada evento de auditoría se registrará, al menos, la siguiente información: fecha/hora del evento, tipo de evento, sujeto identificado (si aplica) y resultado del evento (éxito o fracaso).

25. **REQ. 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.

26. **REQ. 4** El producto deberá disponer de mecanismos apropiados para prevenir la pérdida de registros de auditoría, en el caso de que el espacio para almacenamiento de los registros alcance su límite.

4.2 SOPORTE CRIPTOGRÁFICO

27. **REQ. 5** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).

28. **REQ. 6** 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.

4.3 CANALES CONFIABLES

29. **REQ. 7** 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.).

4.4 SELLADO DE TIEMPO

30. **REQ. 8** El producto debe proporcionar una fuente de tiempo fiable para los registros de auditoría.

4.5 IDENTIFICACIÓN Y AUTENTICACIÓN

31. **REQ. 9** 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.
32. **REQ. 10** El producto deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.

4.6 ADMINISTRACIÓN DE SEGURIDAD

33. **REQ. 11** El producto debe proporcionar un conjunto de funciones de gestión que permitan el control adecuado de sus características y datos.
34. **REQ. 12** El producto debe garantizar que solo los usuarios con los privilegios adecuados puedan ejercer el control de sus funciones y datos.

4.7 SIEM

35. **REQ. 13** El producto deberá ser capaz de recibir, identificar e interpretar eventos procedentes de múltiples fuentes. Debe soportar, al menos, los protocolos: *Syslog* y SNMP (*Simple Network Management Protocol*). También debe ser suficientemente configurable para interpretar y normalizar información procedente de aplicaciones o herramientas propietarias.
36. **REQ. 14** Para la funcionalidad de análisis y correlación de eventos, el producto facilitará la creación de alarmas o notificaciones en el caso de detectar potenciales riesgos para la seguridad.
37. **REQ. 15** Para la funcionalidad de análisis de eventos, el producto deberá ser capaz de analizar los datos recolectados en función de reglas definidas, para identificar usos indebidos o actividades maliciosas, y registrar el resultado de los análisis.
38. **REQ. 16** Para la funcionalidad de análisis de eventos y correlación, el producto debe proteger los eventos almacenados de accesos, modificaciones y borrados no autorizados, así como prevenir la pérdida de eventos por el llenado del espacio de almacenamiento.