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

Noviembre de 2022

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

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2022
NIPO: 083-22-102-1

Fecha de Edición: noviembre de 2022

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.01.03 14:51:30 +01'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

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 y Servicios STIC (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.

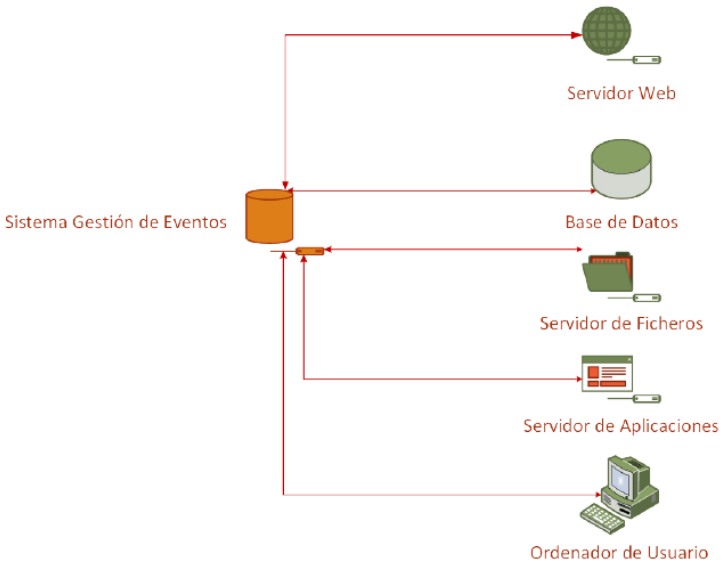

Figura 1. Ejemplo de Caso de Uso 1: Repositorio centralizado de eventos de seguridad

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.

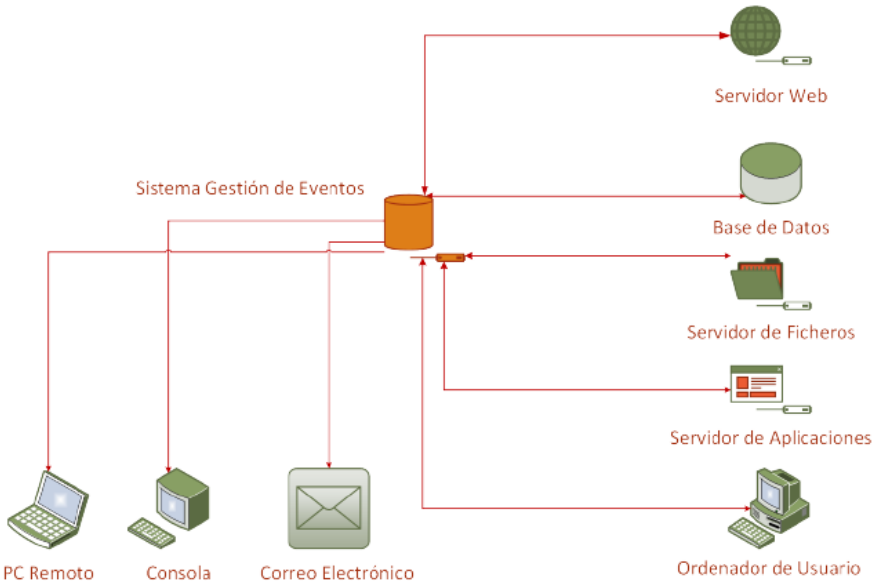

Figura 2. Ejemplo de Caso de Uso 2: Repositorio centralizado y correlación de eventos

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

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 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. En caso de productos software, esta hipótesis aplica a la plataforma física sobre la que se ejecuta el producto.
    - **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.
    - **Actualizaciones periódicas.** El *firmware/software* del producto es actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
    - **Funcionalidad limitada.** El producto solo debe proporcionar la funcionalidad de *Gestión de Eventos* 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.
- **Plataforma confiable**. En caso de tratarse de un producto software, este se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución que la plataforma proporcione.

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 ACTIVOS SENSIBLES A PROTEGER

20. Los recursos a proteger mediante el uso de estos 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.Actualizaciones**. Actualizaciones del producto susceptibles de afectar a su configuración y funcionalidad, que deben ser protegidos en Integridad y Autenticidad.
- **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

21. 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.COM 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.ACT Actualización maliciosa:** un atacante puede realizar una actualización maliciosa que comprometa las funcionalidades 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.INT Compromiso de la integridad del software/firmware:** Un atacante puede intentar comprometer la integridad del producto a través de un software sin privilegios ejecutado en la misma plataforma en la que se ejecuta el producto.
- **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.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.CRE Compromiso de credenciales:** Un atacante puede aprovecharse del uso credenciales débiles o desprotegidas, para ganar acceso privilegiado al producto.

3.3 TRAZABILIDAD AMENAZAS/REQUISITOS DE SEGURIDAD

22. En la siguiente tabla se trazan que Requisitos Fundamentales de Seguridad definidos en el apartado 4 cubren las amenazas definidas:

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.INT	A.PSC	A.NOAUTUSR	A.CRE
ADM.1	X								
ADM2	X								
ADM.3	X								
IAU.1	X							X	
IAU.2									X
IAU.3									X
IAU.4	X								
COM.1		X	X						
COM.2			X						
COM.3			X						
COM.4		X	X						
ACT.1				X					
ACT.2				X					
ACT.3				X					
AUD.1					X				
AUD.2					X				
AUD.3					X				
AUD.4					X				
AUD.5					X				
PSC.1							X		
CIF.1		X	X						
SIEM.1					X				
SIEM.2					X				
SIEM.3					X				
SIEM.4					X				
SIEM.5					X				

4. REQUISITOS DE SEGURIDAD

23. 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.

24. La convención utilizada en las descripciones de los RFS es la siguiente:

- Selección: se deberá seleccionar al menos una opción de las indicadas en el RFS y se incluirá en la declaración de seguridad. Ejemplo:

  RFS: Administración del producto [**selección***: local; remota*]

  DS: Administración del producto local y remota

- Asignación: se deberá especificar el listado de opciones que sean de aplicación al TOE (podría no haber ninguna). Ejemplo:

  RFS: El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación:** otros usuarios del producto] antes de otorgar acceso.

  DS: El TOE deberá identificar y autenticar a cada usuario administrador, auditor y usuario avanzado antes de otorgar acceso.

4.1 ADMINISTRACIÓN CONFIABLE

25. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

26. **ADM.1** El TOE debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.

27. **ADM.2** El TOE debe ser capaz de realizar la gestión de las siguientes funcionalidades:

- Administración del producto [**selección**: *local; remota*].
- Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.
- [**asignación**: otras funcionalidades administrables del producto].

28. **ADM.3** El TOE deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones descritas en **ADM.2**.

> Nota de aplicación: en el caso de que existan distintos tipos de administrador, cada uno de ellos con distintos permisos, deberá probarse que únicamente pueden realizar aquellas funcionalidades para las que tengan permiso.

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

29. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

30. **IAU.1** El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación**: *otros usuarios del producto*] antes de otorgar acceso, salvo para las siguientes funcionalidades [**asignación**: *listado funcionalidades*].

31. **IAU.2** El TOE deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.

32. **IAU.3** El TOE debe disponer de la capacidad de gestión de las contraseñas:

    a) La contraseña debe poder configurarse con una longitud mínima o igual a 12 caracteres.

    b) La contraseña debe ser capaz de componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “].

> Nota de aplicación: este requisito podría ser modificado en el caso de que el TOE implemente otros mecanismos de autenticación.

33. **IAU.4** El TOE debe [**selección***: bloquear; cerrar*] la sesión de un usuario después de [***asignación****: tiempo de inactividad*] de inactividad.

4.3 CANALES CONFIABLES

34. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

35. **COM.1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas: [**selección***: servidor de auditoría;* [***asignación****: otras entidades*]] o entre distintas partes del producto, usando [**selección***: IPSec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación****: listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

36. **COM.2** El TOE debe permitir que los canales de comunicación definidos en **COM.1** sean iniciados por él mismo o por las entidades autorizadas.

37. **COM.3** El TOE hará uso de certificados digitales para la autenticación cuando utilice cualquiera de los protocolos definidos en **COM.1**.

38. **COM.4** Protección de la información del canal de administración. El TOE deberá establecer canales seguros cuando intercambie información con el administrador remoto, usando [**selección**: *IPsec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación****:*

listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo].

4.4 CRIPTOGRAFÍA

39. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

40. **CIF.1** El TOE permitirá exclusivamente el empleo de mecanismos criptográficos: [***asignación**: listado de mecanismos*] autorizados de acuerdo a lo establecido en la guía CCN-STIC-807. La fortaleza de clave empleada será la indicada en esa guía para Categoría MEDIA del ENS, y de acuerdo al nivel de amenaza establecido.

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

41. **ACT.1** El TOE ofrecerá la posibilidad de consultar la versión actual del firmware/software y podrá [**selección**: actualizarse automáticamente; iniciar actualizaciones manualmente] y [**selección**: comprobar si existen nuevas actualizaciones disponibles; ningún otro].

42. **ACT.2** El TOE deberá utilizar [**selección***: hashes publicados; firma digital*] que estén autorizados en la guía CCN-STIC-807 para autenticar las actualizaciones *firmware/software* antes de instalarlas.

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

4.6 AUDITORÍA

44. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

45. **AUD.1** El producto debe generar registros de auditoría cuando se produzca alguno de los siguientes eventos:

    a) Al inicio y finalización de las funciones de auditoría.

    b) *Login* y *logout* de usuarios registrados.

    c) Cambios en las credenciales de usuarios.

    d) Cambios en la configuración del producto [**asignación**: *listado de cambios*].

    e) Eventos relativos a la funcionalidad del producto [**asignación:** *listado de eventos*].

    f) Si el TOE gestiona claves criptográficas, [**selección:** generación; importación; cambio; eliminación de claves criptográficas; ningún otro].

46. **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.

47. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:
    a) Lectura: usuarios autorizados.
    b) Modificación: ningún usuario.
    c) Borrado: [**selección**: solo administradores; ningún usuario]
48. **AUD.4** El TOE debe ser capaz de almacenar en sí mismo la información de auditoría generada y [**selección**: transmitir la información de auditoría generada a una entidad externa utilizando un canal seguro COM.1; no transmitir la información de auditoría generada].
49. **AUD.5** El TOE deberá [**selección**: sobreescribir los registros siguiendo el criterio de mayor antigüedad; enviar a una entidad externa y eliminar; otra opción validada por el CPSTIC] en el caso de que el espacio para almacenamiento de los registros alcance su límite.

4.7 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

50. **PSC.1** En el caso en que el TOE almacene [***selección**: credenciales; claves privadas; [**asignación**: otros parámetros de seguridad críticos*] estos no deberán almacenarse en claro, sino que se utilizarán mecanismos de protección criptológica que cumplan con **CIF.1**.

4.8 SIEM

51. **SIEM.1** El TOE deberá ser capaz de recibir, identificar e interpretar eventos procedentes de múltiples fuentes. Debe soportar, al menos, los protocolos: *Syslog* sobre TLS y SNMP (*Simple Network Management Protocol*). También debe ser suficientemente configurable para interpretar y normalizar información procedente de aplicaciones o herramientas propietarias.
52. **SIEM.2** Para la funcionalidad de análisis y correlación de eventos, el TOE facilitará la creación de [***selección**: alarmas; notificaciones]* en el caso de detectar potenciales riesgos para la seguridad.
53. **SIEM.3** Para la funcionalidad de análisis de eventos, el toe deberá ser capaz de analizar los datos recolectados en función de reglas definidas, para identificar usos indebidos y actividades maliciosas, y registrar el resultado de los análisis.
54. **SIEM.4** Para la funcionalidad de análisis de eventos y correlación, el TOE 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.
55. **SIEM.5** El TOE deberá ser capaz de sellar los registros de auditoria con una fuente de tiempo fiable.

5. ABREVIATURAS

CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
ENS	Esquema Nacional de Seguridad
RFS	Requisitos Fundamentales de Seguridad
TOE	*Target of Evaluation*

PUBLICACIONES DE DEFENSA

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