centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC - Anexo B.9: Sistemas de orquestación, automatización y respuesta de seguridad (SOAR)

Septiembre de 2023

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

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.10.03 16:48:31 +02'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2023

NIPO: 083-23-071-5
Fecha de Edición septiembre de 2023

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 servicio de la familia **Sistemas de orquestación, automatización y respuesta de seguridad (SOAR)** para ser incluido en el apartado de Servicios Cualificados del Catálogo de Productos y Servicios STIC (CPSTIC), publicado por el CCN.
2. Estos requisitos representan las capacidades de seguridad mínimas que cualquier servicio 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 para 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 servicios catalogados dentro de la familia **sistemas de orquestación, automatización y respuesta de seguridad (SOAR)** 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 servicios 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 o servicios asociados a esta familia están orientados a la gestión de incidentes, la automatización de tareas y la coordinación de respuestas. Adicionalmente, proporcionan capacidades de correlación y procesado de alertas, lo que en conjunto permite a las organizaciones una detección y respuesta más rápida a los incidentes de seguridad, minimizando el impacto y mejorando la postura de seguridad global.
7. Son productos o servicios que se conciben como una plataforma de gestión de la seguridad de dispositivos tanto a nivel local, como a través de integraciones con componentes remotos.
8. Estos productos o servicios suelen estar desarrollados por módulos, cada uno de ellos con funciones específicas. Además, pueden contar con agentes que recopilen alertas de forma local o que apliquen las políticas y flujos establecidos desde el servicio principal.
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 registros de alertas 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 registros de alertas de las distintas fuentes. Estos productos o servicios ofrecen una variedad de técnicas de correlación para integrar diferentes fuentes de datos con el fin de convertir los datos en información de calidad para la organización.
    - **Automatización de respuestas**. A partir del análisis de alertas correlacionadas, estos productos o servicios son capaces de permitir la creación de flujos de trabajo y su posterior ejecución automática, lo que mejora la eficiencia y consistencia en la respuesta a incidentes de seguridad.
    - **Repositorio de datos sobre alertas 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 del tipo de despliegue del producto o servicio y de la finalidad o el contexto en que se utilicen, se contemplan dos (2) casos de uso para esta familia de productos, tal y como se definen a continuación.

2.2.1. CASO DE USO 1 – GESTIÓN CENTRALIZADA DE ALERTAS DE SEGURIDAD

11. El servicio es capaz de integrarse de forma directa con distintas fuentes de datos de la organización para maximizar la recepción de información relativa a eventos y alertas. Una vez recopilados los datos, éstos son procesados y almacenados para asegurar su integridad. El producto o servicio también será capaz de integrarse con sistemas de respuesta, para la automatización y ejecución de tareas basándose en la información recolectada.
12. Este caso de uso representará despliegues en los que las comunicaciones podrán ser tanto locales como remotas, pudiendo estos servicios presentar soluciones variadas (*on-premise, cloud, appliance*, etc.).

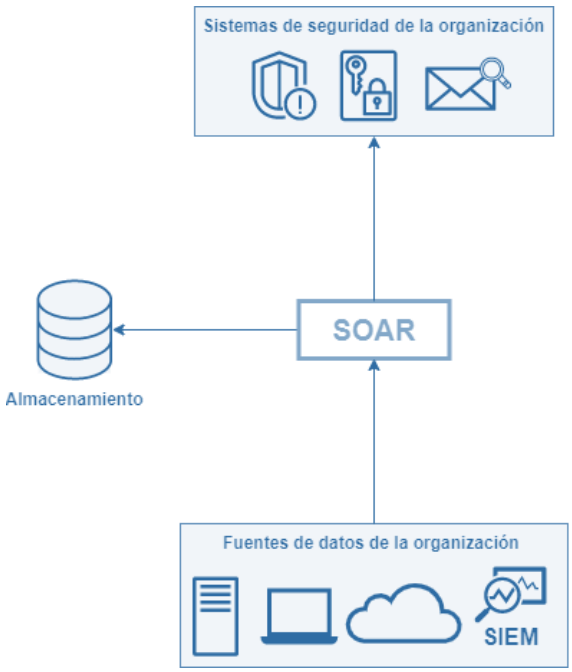

Figura 1 – Ejemplo de Caso de Uso 1: Gestión centralizada de alertas de seguridad.

2.2.2. CASO DE USO 2 – GESTIÓN DE ALERTAS DE SEGURIDAD MEDIANTE AGENTES

13. En este caso se hace uso de agentes como intermediarios para comunicar las fuentes de datos de la organización con el servicio principal. De igual forma, los agentes tendrán la capacidad de comunicarse con los sistemas de seguridad

alojados en la infraestructura de la organización para cumplir la funcionalidad de automatización y respuesta ante incidentes. Para ambas funcionalidades los agentes sincronizarán su configuración con el servicio principal.

14. Este caso de uso será útil en situaciones en las que, por diseño, se decida realizar las comunicaciones entre los servicios de la organización y el agente localmente.

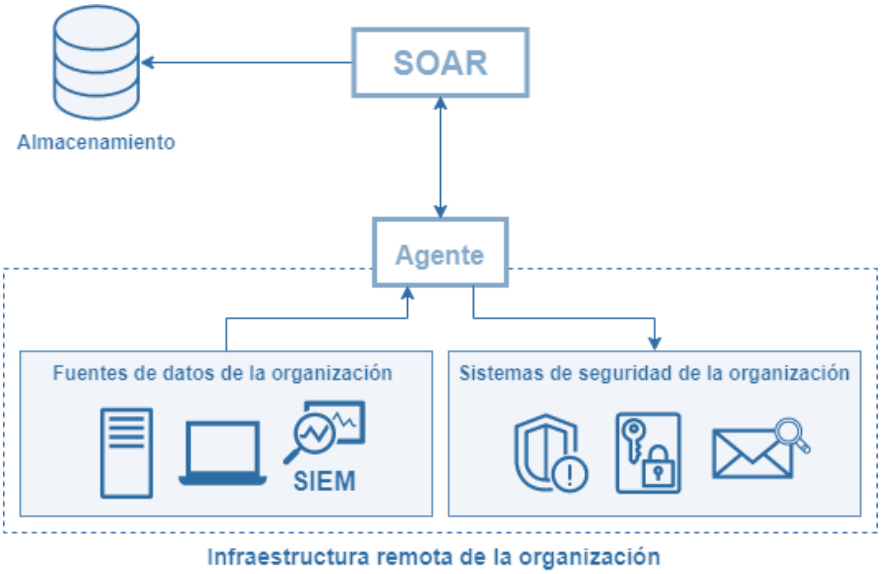

Figura 2 –. Ejemplo de Caso de Uso 2: Gestión de alertas de seguridad mediante agentes.

2.3 ENTORNO DE USO

15. 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 rápida y eficiente respuesta ante posibles incidentes de seguridad, así como el registro de auditoría de seguridad.
16. 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 control de llamadas y transmisión de voz/vídeo, 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

17. Este tipo de productos o servicios se pueden presentar en formato de equipo dedicado (*Appliance*: *hardware* provisto de *firmware* y *software* dedicado) o en forma de servicio en la nube con las funcionalidades estrictamente necesarias para cumplir su finalidad y acotadas al servicio específico que presten.

18. En el caso de gestión de alertas de seguridad mediante agentes, los agentes se presentan en forma de aplicación *software* que se ejecuta sobre un Sistema Operativo de propósito general.

19. 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 ALINEAMIENTO CON CRITERIOS COMUNES (*COMMON CRITERIA*)

20. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TIC (Tecnologías de la Información y de las Comunicaciones).

21. 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.

22. Los productos dentro de esta familia deberán estar certificados de acuerdo a la norma *Common Criteria.* Dicha certificación deberá evidenciar el problema de seguridad definido en el presente documento e incluir los requisitos fundamentales de seguridad recogidos en el apartado 4.

23. El nivel de confianza EAL (*Evaluation Assurance Level*) con el que deben ser evaluados los requisitos exigidos para esta familia será EAL2 o superior.

24. En caso de que alguno de los requisitos indicados en el apartado 4 no se encuentre recogido en la declaración de seguridad del producto, pero este sí implemente esa función de seguridad, se podrá llevar a cabo una evaluación **STIC complementaria**, cuyo objetivo será verificar el cumplimiento de esos requisitos.

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

25. Los recursos que deben protegerse 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 de 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

26. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente, atendiendo a los casos de uso expuestos en la sección 2.2, 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.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.FUN Fallo de las funcionalidades de seguridad**: Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad declaradas del producto y podría acceder, cambiar o modificar información, funcionalidades de seguridad o tráfico de red en el producto.
- **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.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

27. 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.

28. 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 AGENTE

29. Los requisitos incluidos en este apartado aplican al agente para el caso de uso 2 – gestión de alertas de seguridad mediante agentes.

4.1.1. PERFIL DE PROTECCIÓN

AG.CER.1 El agente 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**
Protection Profile for Application Software.[1]	1.3	01/03/2019	NIAP
Protection Profile for Application Software.[2]	1.2	25/04/2016	NIAP

Tabla 1. Perfiles de protección *Application Software*

AG.CER.2 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 *Protection Profile for Application Software V.1.3* con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

[1] https://www.commoncriteriaportal.org/files/ppfiles/pp_app_v1.3.pdf
[2] https://www.commoncriteriaportal.org/files/ppfiles/pp_app_v1.2.pdf

4.1.2. CANALES SEGUROS

AG.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*].

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

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

4.2 SERVIDOR

30. Los requisitos incluidos en este apartado aplican a la parte de servidor:

4.2.1. ADMINISTRACIÓN CONFIABLE

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

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*].

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.

4.2.2. IDENTIFICACIÓN Y AUTENTICACIÓN

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*].

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

IAU.3 El TOE deberá 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.

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

IAU.5 Cuando el acceso se realice utilizando credenciales por defecto o el usuario no tenga asignadas credenciales, el TOE obligará al [**selección***: cambio; establecimiento*] de credenciales en el siguiente acceso.

4.2.3. CANALES SEGUROS

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*].

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.

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

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*].

4.2.4. AUDITORÍA

31. Podrán ser cubiertas por el producto o por su entorno operacional.

AUD.1 El TOE debe generar registros de auditoría y cuando se produzca alguno de los siguientes eventos:

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

b) *Login* y *logout* de usuarios.
c) Cambio 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*].

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.

AUD.3 A los registros de auditoría se aplicará la siguiente política de acceso:

a) Lectura: solo usuarios autorizados.

b) Modificación: ningún usuario.

c) Borrado: [**selección***: solo administradores; ningún usuario*]

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*].

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.

4.2.5. PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

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.

4.2.6. CRIPTOGRAFÍA

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 ALTA del ENS, y de acuerdo al nivel de amenaza establecido.

4.3 SOAR

Nota: Los requisitos propios de este apartado hacen uso del término “alerta”. Éste es empleado teniendo en cuenta la siguiente definición:
Alerta: datos en bruto recibidos por el producto que serán eventos correlacionados, alarmas o datos equivalentes.

SOAR.1 El TOE deberá ser capaz de recibir, identificar e interpretar alertas procedentes de múltiples fuentes. También debe ser suficientemente configurable para interpretar y normalizar alertas procedentes de aplicaciones o herramientas propietarias.

SOAR.2 Para la funcionalidad de correlación de alertas, el TOE deberá ser capaz de procesar los datos recolectados en función de reglas definidas, permitiendo [**selección**: *buscar atributos comunes; relaciones; ningún otro*] entre los registros de alertas.

SOAR.3 El TOE deberá ser suficientemente configurable para integrarse con aplicaciones o herramientas externas, permitiendo la ejecución de acciones de respuesta de forma [**selección:** *manual; automática*].

SOAR.4 Para la funcionalidad de automatización de respuestas, el TOE deberá permitir la creación de reglas que provoquen el inicio de la ejecución de tareas.

SOAR.5 Para la funcionalidad de automatización de respuestas, el TOE deberá permitir la creación de flujos de tareas que se ejecuten atendiendo a las reglas definidas en **SOAR.4**.

SOAR.6 En caso de que el TOE se comunique con entidades externas, este únicamente enviará aquella información que haya sido declarada por el fabricante y no contendrá datos personales. El producto no establecerá conexiones de red no declaradas.

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*
SOAR	*Security Orchestration, Automation and Response.*
TIC	Tecnologías de Información y las comunicaciones.
TOE	*Target of Evaluation*

PUBLICACIONES
Pd
DE DEFENSA

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