centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo F.9-M: Herramientas CASB

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

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
2023.01.03 14:53:36 +01'00'

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

Fecha de Edición: noviembre de 2022

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 **Herramientas CASB** 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) para 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 ***Herramientas CASB*** 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 la familia Herramientas CASB (*Cloud Access Security Broker*) surgen para dar respuesta a la necesidad de visibilidad y control sobre el uso que hacen los usuarios de una organización de las aplicaciones y servicios en la nube.
7. Hace años, las organizaciones utilizaban estos productos para localizar lo que se denomina TI oculta (*shadow IT*), es decir, aquellas aplicaciones en la nube no autorizadas, a las que los usuarios acceden sin conocimiento de la organización.
8. Hoy en día, los productos CASB se utilizan para minimizar las amenazas de seguridad a las que las organizaciones están expuestas cuando utilizan aplicaciones y recursos en la nube. Representan un punto central en el que la organización puede implementar políticas de seguridad que regulen el uso que realizan usuarios y dispositivos, de aplicaciones y servicios en la nube.
9. Algunas de las características de estos productos son las siguientes:

    - **Visibilidad de aplicaciones en la nube.** Detectan, de forma automática y continua, las aplicaciones y servicios en la nube que están utilizando los usuarios. Tanto aquellas aplicaciones permitidas, como las no autorizadas (*shadow IT*).
    - **Detección, clasificación y prevención contra fugas de datos.** Pueden identificar, clasificar e inspeccionar datos sensibles o sujetos a regulación, que se estén intercambiando o almacenando en la nube.
    - **Gestión de cuentas de usuarios.** Pueden identificar cuentas inactivas, cuentas huérfanas o cuentas de usuarios externos.
    - **Indicadores de riesgo.** Pueden crear indicadores detallados de la postura en materia de riesgos de las aplicaciones en la nube, pudiendo incluir ponderaciones personalizadas.
    - **Políticas personalizadas.** Creación de políticas de seguridad personalizadas, basadas en diversos atributos. Pueden generar notificaciones en tiempo real sobre violaciones de las políticas.
    - **Monitoreo y análisis en tiempo real,** de las actividades realizadas por los usuarios en la nube.
    - **Detección automática de anomalías.** A través de la monitorización continua, pueden detectar conductas y actividades anómalas, que identifiquen empleados de alto riesgo y ataques externos.
    - **Prevención contra amenazas en tiempo real.** Pueden correlar las anomalías detectadas en la actividad con otros datos considerados de

riesgo (por ejemplo, direcciones IP) y aplicar políticas para alertar, bloquear, poner en cuarentena, etc.

- **Configuraciones de seguridad.** Pueden comparar las configuraciones de seguridad de las aplicaciones en la nube con un conjunto de mejores prácticas y requisitos mínimos de seguridad impuestos por la legislación aplicable.
- **Integración con otras herramientas corporativas,** como SIEM, *firewalls*, herramientas EPP/EDR, LDAP, MDM, etc.

2.2 CASOS DE USO

10. Dependiendo de las funcionalidades y características de despliegue del producto, se contemplan tres (3) casos de uso para esta familia de productos, tal y como se definen a continuación.

2.2.1. CASO DE USO 1 – MODO API (FUERA DE LÍNEA)

11. En el modo API o "fuera de línea", el producto hace uso de las API proporcionadas por el proveedor cloud (CSP), para conocer la actividad de los usuarios de la organización. El producto no solo se comunica con los equipos de usuario, sino también con otras fuentes de información de la red corporativa (como firewalls).
12. La ventaja del modo API o "fuera de línea" es la visibilidad que proporciona sobre las aplicaciones en la nube que están usando los usuarios. Proporciona incluso visibilidad "este-oeste", es decir, de aquellas aplicaciones de una nube secundaria a las que el usuario está accediendo a través de la nube principal.

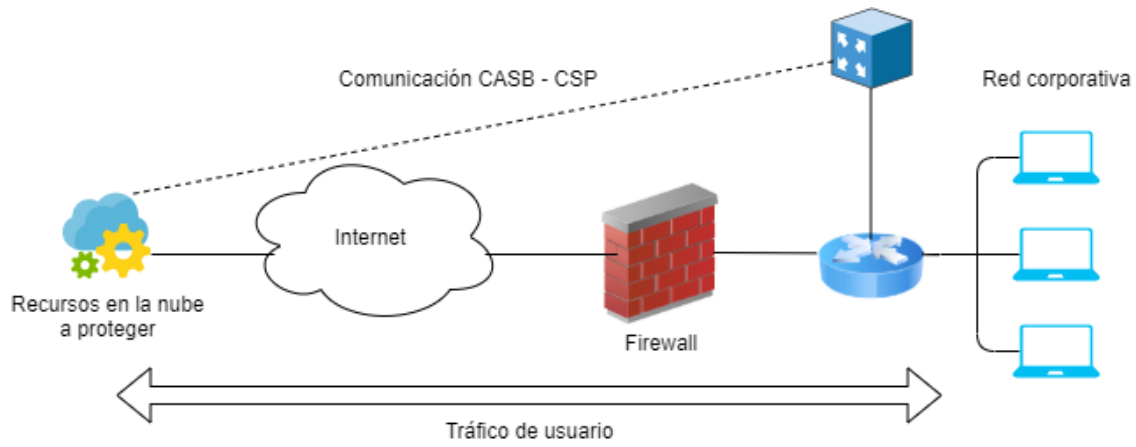

Figura 1 – Ejemplo de Caso de Uso: Modo API (fuera de línea)

2.2.2. CASO DE USO 2 – MODO *PROXY* (EN LÍNEA)

13. En el modo *Proxy* o "en línea" el producto se instala como un *proxy*, utilizando alguno de los elementos de red de la organización, de forma que todo el tráfico entre los usuarios y la nube pasa a través de él. Puede operar como *proxy* inverso, o *proxy* directo (instalando un agente en el equipo de usuario).
14. La ventaja de la configuración Proxy o "en línea" es la capacidad de actuación (*enforcement*) de las políticas de seguridad implementadas, actuando directamente sobre lo que los usuarios pueden hacer o no respecto a la nube.

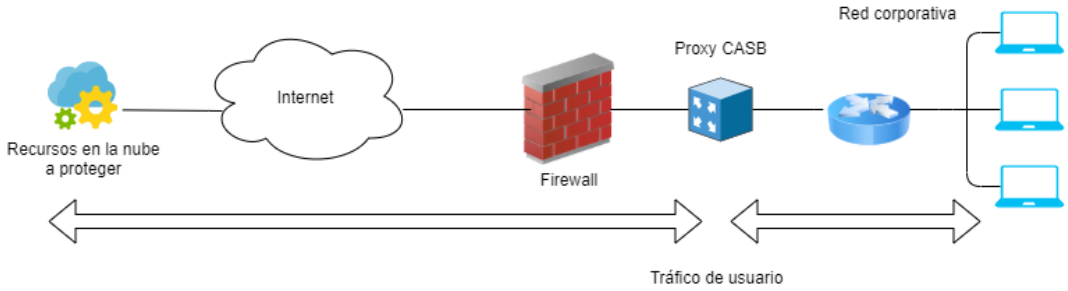

Figura 2 – Ejemplo de caso de uso: Modo Proxy (en línea)

2.2.3. CASO DE USO 3 – MODO MIXTO

15. Algunos productos CASB disponen de ambas configuraciones. Esto permite que, en primer lugar, se utilice la configuración "fuera de línea" (API) para maximizar el descubrimiento de aplicaciones, investigar el panorama de amenazas, y crear, en consecuencia, las políticas de seguridad más apropiadas. Posteriormente, se activa el modo "en línea" (*proxy*) para aplicar esas políticas de la forma más eficaz.

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

16. Para la utilización en condiciones óptimas de seguridad de los sistemas para la prevención de fuga de datos, es necesario que se integre en un entorno de trabajo que cumpla una serie de 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 *Sistemas de prevención de fuga de datos* 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. Estos productos pueden constar de uno o varios componentes, los cuales pueden presentarse tanto en formato Equipo dedicado o *Appliance* (*hardware* provisto de firmware dedicado y *software*), como en forma de aplicación *software*. En este caso, podrían consistir en *software* instalado en equipos dentro de la red empresarial, o en aplicaciones SaaS (*Software-as-a-Service*).

2.5 CERTIFICACIÓN LINCE

18. Para que un producto de esta familia pueda ser incluido en el CPSTIC bajo la categorización de ENS Categoría 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.
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) y de Evaluación Criptográfica (MEC) serán opcionales.

[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 que es necesario proteger mediante el uso de esta familia de 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.
- **A.CASB. Acceso a información sensible**. Un atacante consigue acceder de forma no autorizada a las aplicaciones o servicios en la nube de la organización, accediendo a información sensible.

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	A.CASB
ADM.1	X									
ADM2	X									
ADM.3	X									
IAU.1	X							X		
IAU.2									X	
IAU.3									X	
IAU.4	X									

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.INT	A.PSC	A.NOAUTUSR	A.CRE	A.CASB
IAU.5									X	
COM.1		X	X							
COM.2			X							
COM.3			X							
COM.4		X	X							
ACT.1				X						
ACT.2				X						
ACT.3				X						
ACT.4				X						
ACT.5				X						
AUD.1					X					
AUD.2					X					
AUD.3					X					
AUD.4					X					
AUD.5					X					
EXP.3						X				
PSC.1							X			
CIF.1		X	X							
CASB.1										X
CASB.2										X
CASB.3										X
CASB.4										X
CASB.5										X
CASB.6										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.

34. **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.

4.3 CANALES SEGUROS

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

36. **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*].

37. **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.

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

39. **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

40. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
41. **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

42. **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].
43. **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.
44. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.
45. **ACT.4** En el caso de que el TOE sea una *aplicación software*, esta deberá estar empaquetada de forma que, si se elimina, no deje rastro de su instalación (excepto por configuraciones y ficheros de salida o auditoría).
46. **ACT.5** En el caso de que el TOE sea una *aplicación software*, este no descargará ni modificará su propio código binario.

4.6 AUDITORÍA

47. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
48. **AUD.1** El TOE 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].

49. **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.

50. **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]

51. **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].

52. **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 CAPACIDADES ANTI-EXPLOTACIÓN

53. **EXP.3** En el caso de que el TOE sea una aplicación *software*, este solamente utilizará las bibliotecas de terceras partes declaradas [**asignación***: listado de librerías*].

4.8 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

54. **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**.

4.9 REQUISITOS CASB

55. **CASB.1.** El TOE debe detectar todas las aplicaciones y servicios autorizados en la nube que están siendo usados por los empleados de la organización, incluidos aquellos servicios en la nube no autorizados (*Shadow IT)*: [**asignación:** *listado de servicios y aplicaciones detectados por el TOE*].

56. **CASB.3.** El TOE debe permitir la aplicación de políticas para proteger los datos de la organización en la nube. Esto implica, al menos, un control de acceso granular y mecanismos para impedir la carga de datos en la nube que no cuenten con

autorización para ello, de acuerdo políticas de seguridad establecidas por la organización.

57. **CASB.4.** El TOE debe monitorizar la actividad realizada sobre las aplicaciones y servicios en la nube. En concreto, debe detectar actividad anómala y archivos sospechosos. Debe proporcionar mecanismos que mitiguen las amenazas e impidan la propagación de *malware*, como entornos *sandbox* para análisis dinámico o implementando flujos de cuarentena para los ficheros sospechosos.

58. **CASB.5.** El TOE debe llevar un registro de los usuarios que acceden a las aplicaciones y servicios en la nube. Debe detectar aquellos usuarios que llevan mucho tiempo inactivos, así como los usuarios externos a la organización (consultores externos, proveedores, etc.).

59. **CASB.6.** El TOE debe registrar las actividades realizadas por los usuarios sobre las aplicaciones y servicios en la nube. Se debe registrar fecha y hora de acceso, dirección IP, ubicación geográfica, actividad, servicio o aplicación, usuario y [**asignación:** *listado de campos adicionales*].

4.10 NOTAS DE APLICACIÓN GENERALES

60. En caso de que el producto no implemente la funcionalidad a la que aplica alguno de los requisitos anteriores (o algunas partes de ellos), y ésta sea proporcionada por el entorno operacional, el fabricante deberá indicarlo en la declaración de seguridad o justificarlo debidamente. En este caso, se considerará que el requisito ***no aplica***.

61. Lo anterior no es válido en caso de que tal funcionalidad solicitada en un requisito, sea proporcionada por un componente del producto que no forma parte de la configuración evaluada. En este caso ***sí aplica***, y el fabricante deberá demostrar el correcto cumplimiento del requisito por parte del producto.

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*
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