centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

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

Abril 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

NIPO: 083-19-053-9.

Fecha de Edición: abril de 2020

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 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 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.

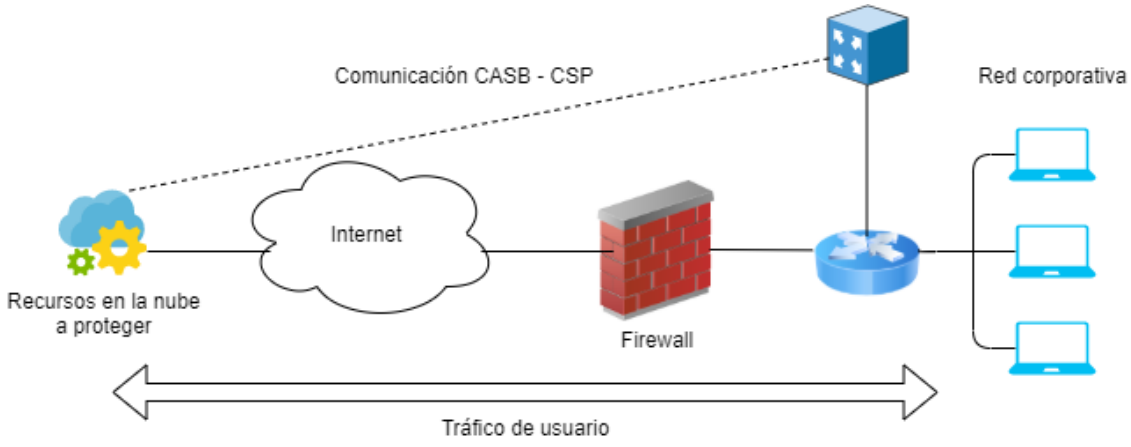

Figura 1 – Ejemplo de Caso de Uso: Modo API (fuera de línea)

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.

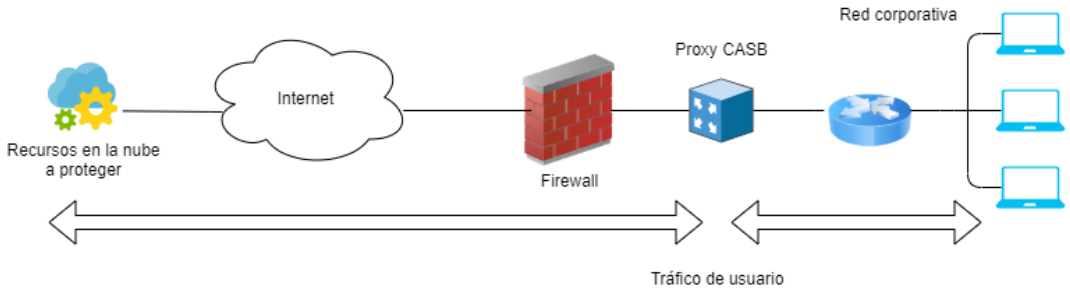

Figura 2 – Ejemplo de caso de uso: Modo Proxy (en línea)

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 ENTORNO DE USO

16. Para la utilización en condiciones óptimas de seguridad de la herramienta CASB, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

    - **Protección física:** En caso de que el producto contenga componentes a instalar en la red de la organización, dichos componentes deberán instalarse en un área donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.
    - **Administración confiable:** El Administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la empresa/administración. Por ello, se asume que dicha persona estará capacitada, formada y carecerá de cualquier intención dañina al administrar el producto.

- **Actualizaciones periódicas:** El *firmware* y el *software* del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **Política de Seguridad de la Información:** La política de seguridad deberá recoger el conjunto de principios, la organización y los procedimientos impuestos por una organización para hacer frente a sus necesidades de seguridad de la información, incluyendo el uso de las TIC.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

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 ALINEAMIENTO CON CRITERIOS COMUNES (*COMMON CRITERIA*)

18. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos TIC (Tecnologías de la Información y de las Comunicaciones).
19. En el ámbito de CC se definen un conjunto de objetivos y requisitos de seguridad, tanto funcionales (*SFR, Security Functional Requirements*) como de evaluación (*SAR, Security Assurance Requirements*), independientes de la implantación, que cada producto incluirá dentro de su declaración de seguridad (*ST, Security Target*).
20. **Los productos dentro de esta familia, deberán disponer de una declaración de seguridad (ST) certificada con un nivel de confianza EAL2 o superior (*Evaluation Assurance Level*), que contenga los SFR indicados en el apartado 4.**
21. En caso de que alguno de los requisitos indicados en la tabla anterior 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

22. Los recursos que es necesario proteger mediante el uso de esta familia de productos, incluyen:

- Comunicaciones con el producto.
- 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.
- Información de la organización almacenada en el producto.

3.2 AMENAZAS

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

- **A.RED. Ataque a la red.** Un atacante, desde dentro o desde fuera de la red, consigue acceder y/o modificar la información intercambiada entre el producto y otras entidades autorizadas o entre los distintos módulos del producto.
- **A.LOCAL. Ataque local.** Un atacante puede actuar a través de *software* no privilegiado ejecutado en la misma plataforma de computación donde se ejecuta el producto. Los atacantes podrían modificar de forma maliciosa los ficheros o comunicaciones que utiliza el producto.
- **A.REST. Acceso a información almacenada.** Un atacante puede acceder a información sensible almacenada en la plataforma en la que se instala y ejecuta el producto.
- **A. SEG. Acceso a las funciones de seguridad.** Un atacante podría acceder y modificar las funciones y datos de seguridad del producto.
- **A.NODET. Actividad no detectada.** Un atacante consigue acceder, cambiar o modificar la funcionalidad de seguridad de la herramienta sin que esto sea apreciado por el administrador.
- **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.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

24. 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 ADMINISTRACIÓN CONFIABLE

25. Estas funcionalidades de seguridad mitigan la amenaza (A.SEG). **Podrán ser cubiertas por el producto o por su entorno operacional.**
26. **ADM.1** El producto debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.
27. **ADM.2** El producto debe ser capaz de realizar la gestión de las siguientes funcionalidades:
    - Administración del producto de forma local (en caso de que se instale dentro de la red de la organización) y remota.
    - Configuración del tiempo de terminación de sesión o bloqueo, al detectar inactividad.
    - Otros parámetros de configuración del producto.
28. **ADM.3** El producto deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones anteriormente descritas (ADM.2).

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

29. Estas funcionalidades de seguridad mitigan la amenaza (A.REST, A.SEG). **Podrán ser cubiertas por el producto o por su entorno operacional.**
30. **IAU.1.** El producto deberá identificar y autenticar a cada usuario antes de otorgar acceso.
31. **IAU.2.** El producto deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
32. **IAU.3.** El producto deberá proteger de lectura y modificación no autorizada las credenciales de autenticación.
33. **IAU.4.** El producto 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 [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “]

34. **IAU.5.** El producto debe bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad.

4.3 AUDITORÍA

35. Estas funcionalidades de seguridad mitigan la amenaza (A.NODET).
36. **AUD.1.** El producto deberá generar registros de auditoría al comienzo y finalización de las funciones de auditoría y cuando se produzca alguno de los siguientes eventos:
    a) Login y logout de personal autorizado.
    b) Cambios en la configuración de usuarios.
    c) Cambios en la configuración del producto.
    d) Eventos relativos a la funcionalidad del producto
37. **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 (si aplica).
38. **AUD.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.
39. **AUD.4.** Si se trata de un producto *appliance*, debe ser capaz de almacenar la información de auditoría generada en sí mismo o en una entidad externa.
40. **AUD.5.** Si se trata de un producto *appliance*, este debe ser capaz de eliminar o sobrescribir registros de auditoría anteriores cuando el espacio de almacenamiento esté lleno.

4.4 CANAL SEGURO

41. Estas funcionalidades de seguridad mitigan la amenaza (A.RED).
42. **COM.1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas o entre distintas partes del producto empleando funciones, algoritmos y protocolos que estén de acuerdo con lo establecido en la guía CCN-STIC-807 (p.ej.: HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, etc.).
43. **COM.2** El TOE debe permitir que estos canales de comunicación seguros sean iniciados por él mismo o por entidades autorizadas.
44. **COM.3** El producto hará uso de certificados digitales para la autenticación cuando utilice cualquiera de estos protocolos.

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

45. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL, A.SEG).
46. **ACT.1** El producto ofrecerá la posibilidad de consultar la versión actual del *firmware/software*, iniciar actualizaciones manualmente y comprobar si existen nuevas actualizaciones disponibles.
47. **ACT.2** El producto deberá ofrecer mecanismos, conforme a la criptografía de empleo en el ENS, a través de hashes o firma digital para autenticar las actualizaciones de *firmware/software* antes de instalarlas.
48. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.
49. **ACT.5**En caso de tratarse de un producto *software*, este deberá estar empaquetado de forma que, si se elimina, no deje rastro de su instalación (excepto por configuraciones y ficheros de salida o auditoría).
50. **ACT.6** En caso de tratarse de un producto *software*, este no descargará ni modificará su propio código binario.
51. **ACT.7** En caso de tratarse de un producto *software*, solamente utilizará las bibliotecas de terceras partes declaradas por el fabricante.

4.6 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

52. Estas funcionalidades de seguridad mitigan la amenaza (A.REST). **Podrán ser cubiertas por el producto o por su entorno operacional.**
53. **CRD.1.** En el caso en que el producto almacene credenciales y/o datos sensibles, éstos no deberán almacenarse en claro.

4.7 REQUISITOS CRIPTOGRÁFICOS

54. Estas funcionalidades de seguridad mitigan las amenazas (A.RED, A.REST).
55. **CIF.1** El TOE permitirá exclusivamente el empleo de funciones, algoritmos y protocolos criptográficos que estén incluidas entre las autorizadas para categoría ALTA del ENS, de acuerdo a lo establecido en la guía CCN-STIC-807.
56. **CIF.2** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).

4.8 REQUISITOS CASB

57. Estas funcionalidades de seguridad mitigan las amenazas (A.CASB).

    CASB.1. El producto 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*).

58. **CASB.3.** El producto 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.

59. **CASB.4.** El producto 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.

60. **CASB.5.** El producto 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.).

61. **CASB.6.** El producto debe registrar las actividades realizadas por los usuarios sobre las aplicaciones y servicios en la nube. Al menos, debe registrar fecha y hora de acceso, dirección IP y ubicación geográfica, y detectar accesos sospechosos y el usuario que los causó.

4.9 NOTAS DE APLICACIÓN

62. 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***.

63. 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*