centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC-
Anexo A7: Gestión de Identidades (IM)

Agosto 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN 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
2020.08.10 10:19:20 +02'00'

NIPO: 083-19-053-9.

Fecha de Edición: Agosto 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 **Gestión de Identidades (IM, *Identity Management*)** 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 **Gestión de Identidades (IM)** 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 de Gestión de Identidades (*IM, Identity Management)* surgen para dar respuesta a la necesidad que tienen las organizaciones de disponer de servicios centralizados y sincronizados de identidades digitales, que permitan gestionar usuarios con atributos y credenciales asociados y la aplicación de políticas de gestión centralizada.

7. En los últimos años, muchas organizaciones han crecido de manera descontrolada y no cuentan con tiempo ni recursos suficientes, para gestionar de manera apropiada y centralizada sus usuarios y los privilegios que deberían tener para desarrollar sus actividades. Esto puede derivar en brechas de seguridad que pueden dar lugar a vulnerabilidades en la organización.

8. Hoy en día, los productos de Gestión de Identidades se utilizan para generar una identidad única para cada usuario, de manera que se le pueda identificar de manera unívoca y asociar el resto de atributos para la autenticación (credenciales) y autorización (permisos), junto con otros atributos de interés. El Gestor de Identidades representa la autoridad respecto a los datos de identidad y credenciales de usuarios. Los define, mantiene y transmite de forma segura a otros componentes del entorno.

9. Algunas de las características de estos productos son las siguientes:

   - **Aprovisionamiento de usuarios.** Consiste en la creación y gestión de nuevos usuarios con sus respectivos atributos, en un repositorio corporativo, así como la asociación o eliminación de atributos a un determinado usuario.
   - **Servicios de sincronización.** Sincronización automática mediante canales seguros, de la información de identidades entre los diferentes componentes que hacen uso de dicha información.
   - **Gestión del ciclo de vida de las credenciales de los usuarios.** Emisión y mantenimiento de las credenciales a lo largo de su ciclo de vida, que podrán pasar por varios estados como: *activación, suspensión* y *finalización.*
   - **Auditoría.** Generación de registros de auditoría que recojan todas las acciones realizadas sobre la información de identidades y credenciales, y procesos de autenticación en el producto.
   - **Configuración de políticas de contraseñas** aplicables a las credenciales de los usuarios. Estas serán configuradas por los administradores siguiendo las políticas de la organización.

2.2 CASOS DE USO

10. Dada la naturaleza y el objetivo de este tipo de productos, se contemplan dos casos de uso para esta familia tal y como se indica a continuación.

2.2.1. CASO DE USO 1 – GESTOR DE IDENTIDADES Y CREDENCIALES CON ALMACENES DE DATOS PROPIOS

11. En este caso de uso, el producto realiza la gestión, almacenamiento y distribución de la información de identidades y credenciales. Cuenta con sus propias bases de datos locales para el almacenamiento de la información de identidades, credenciales, atributos y registros de auditoría.
12. El producto provisiona, a través de conectores, la información de identidad y credenciales a otros productos del entorno con los que interactúa, como servidores de autenticación, control de accesos, gestores de configuración o gestor de políticas.

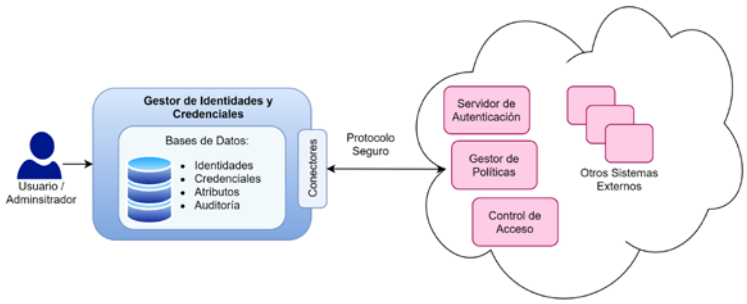

Figura 1 – Caso de Uso Gestor de Identidades y Credenciales con almacenes de datos propios.

2.2.2. CASO DE USO 2 – GESTOR DE IDENTIDADES Y CREDENCIALES SIN ALMACENES DE DATOS PROPIOS

13. En este caso de uso, el producto realiza la gestión y la distribución de la información de identidades y credenciales. El producto interactúa con los almacenes de datos ya existentes en la organización y que forman parte del entorno operacional, en lugar de proporcionar los suyos propios.
14. El producto provisiona, a través de conectores, de la información de identidad y credenciales a otros productos del entorno con los que interactúa, como servidores de autenticación, control de accesos, gestores de configuración o gestor de políticas.

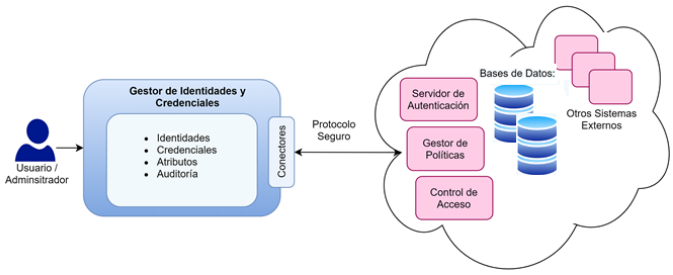

Figura 2 – Caso de Uso Gestor de Identidades y Credenciales sin almacenes de datos propios.

2.3 ENTORNO DE USO

15. Para la utilización en condiciones óptimas de seguridad de la herramienta de Gestión de Identidades, 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:** Los administradores serán miembros de plena confianza y que velan por los mejores intereses en materia de seguridad de la organización. Dichas personas deberán estar debidamente capacitadas y carecerán de cualquier intención maliciosa o conflicto de intereses al administrar el producto.
    - **Plataforma segura:** En caso de tratarse de un producto software, este se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.
    - **Actualizaciones periódicas:** El *firmware* (si aplica) y el *software* del producto serán actualizados conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
    - **Entidades de terceros confiables:** En caso de que la información de identidades, atributos y credenciales, sea intercambiada con entidades de terceros, estas deberán ser de confianza.
    - **Servicios internos:** En algunos casos, el producto puede requerir que el entorno operacional proporcione determinados servicios, dentro de la red interna en la que se despliega el producto, como pueden ser:
        - Bases de datos repositorio de información de identidades, atributos y credenciales.
        - Servidores de auditoría y de autenticación.
        - Gestores de políticas, de configuración y de control de acceso.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

16. Este tipo de productos se presentan en formato *software*, instalándose en un sistema de ficheros proporcionado por un sistema operativo. Se ejecuta en una plataforma que puede ser el sistema operativo, un entorno de ejecución o una combinación de las anteriores.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (*COMMON CRITERIA*)

17. 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).
18. 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.
19. 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.
20. El nivel de confianza EAL (*Evaluation Assurance Level*) con el que deben ser evaluados los requisitos exigidos para esta familia será:
    - **El determinado por el perfil de protección** para aquellos SFR incluidos en los perfiles exigidos cuando los productos se encuentren certificados contra alguno de los perfiles anteriormente descritos.
    - **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra ningún perfil.
21. 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

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

- AC Administración. Interfaces de gestión del producto e información transmitida a través de ellas, en ambos sentidos.
- AC Datos. Datos de configuración del producto y de auditoría generados por éste. Información que atraviese el producto entre sus interfaces de red. Datos de identidades, atributos y credenciales de usuario gestionados y almacenados por el producto.
- AC. Actualizaciones. Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

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.INSUF_ATRB. Atributos insuficientes**. El producto no permite definir identidades, credenciales y atributos con detalle suficiente para posibilitar que las funciones de autenticación y control de acceso se realicen de forma eficaz. Esto puede causar que otros productos relacionados con el control de acceso (gestor de políticas de seguridad, control de acceso, servidor de

autenticación, etc.), se comporten de forma ineficaz permitiendo accesos y actividades ilegítimas.

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 PERFIL DE PROTECCIÓN COMMON CRITERIA

25. **REQ. 1.** Los productos deberán estar certificados con el siguiente perfil de protección de acuerdo a la norma *Common Criteria*:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Enterprise Security Management - Identity and Credential Management [1]	*2.1*	*21/11/2013*	*NIAP*

Tabla 1. Perfiles de Protección.

26. **REQ. 2.** En caso de que el producto no esté certificado contra el perfil anterior, debe disponer de una declaración de seguridad (*Security Target*) certificada con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**. La declaración de seguridad debe contener los SFR (*Security Functional Requirements*) del perfil de protección *Protection Profile for Enterprise Security Management - Identity and Credential Management v2.1*.

4.2 REQUISITOS CRIPTOGRÁFICOS

27. **REQ.3** El producto 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.

[1] https://www.niap-ccevs.org/MMO/PP/pp_esm_icm_v2.1.pdf

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
ESM	*Enterprise Security Management*
NIAP	*National Information Assurance Partnership*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*
TOE	*Target of Evaluation*