centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC-
Anexo A.7-M: 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 10:18:34 +02'00'

NIPO: 083-19-053-9.

Fecha de Edición: Agosto 2020

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) 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 **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

1. 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.
2. 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.

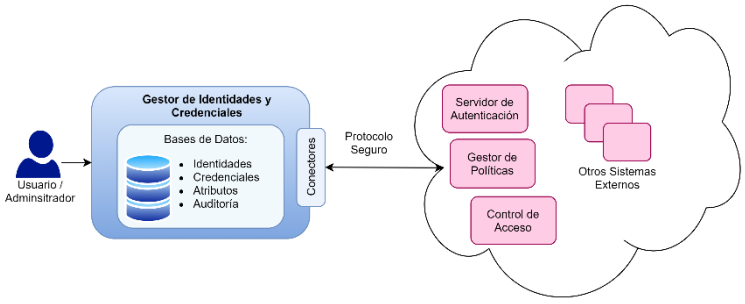

Figura 1 – Caso de Uso Gestor de Identidades y Credenciales con almacenes de datos propios.

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

3. 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.
4. 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.

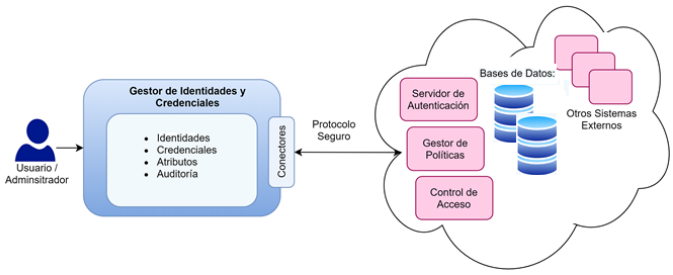

Figura 2 – Caso de Uso Gestor de Identidades y Credenciales sin almacenes de datos propios.

2.3 ENTORNO DE USO

5. 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

6. 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 CERTIFICACIÓN LINCE

7. 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, que deberán ser 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 RECURSOS QUE ES NECESARIO PROTEGER

8. 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/o almacenados por el producto.
   - AC. Actualizaciones. Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

9. 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)

10. 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

11. Estas funcionalidades de seguridad mitigan la amenaza (A.SEG). **Podrán ser cubiertas por el producto o por su entorno operacional.**
12. **ADM.1** El producto debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.
13. **ADM.2** El producto debe ser capaz de realizar la gestión de las siguientes funcionalidades:
    - Administración del producto de forma local y remota.
    - Configuración del tiempo de terminación de sesión o bloqueo, al detectar inactividad.
    - Otros parámetros de configuración del producto.
14. **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

15. Estas funcionalidades de seguridad mitigan la amenaza (A.REST, A.SEG). **Podrán ser cubiertas por el producto o por su entorno operacional.**
16. **IAU.1.** El producto deberá identificar y autenticar a cada usuario antes de otorgar acceso.
17. **IAU.2.** El producto deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
18. **IAU.3.** El producto deberá proteger de lectura y modificación no autorizada las credenciales de autenticación.
19. **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 [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “]

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

4.3 AUDITORÍA

21. Estas funcionalidades de seguridad mitigan la amenaza (A.NODET). Podrán ser cubiertas por el producto o por su entorno operacional.
22. **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 las credenciales y atributos de usuarios.
    c) Cambios en la configuración del producto.
    d) Eventos relativos a la funcionalidad del producto
23. **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).
24. **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: solo administradores.
25. **AUD.4**. El producto debe ser capaz de almacenar la información de auditoría generada en sí mismo o en una entidad externa.
26. **AUD.5**. El producto debe ser capaz de eliminar o sobrescribir registros de auditoría anteriores cuando el espacio de almacenamiento esté lleno.

4.4 CANAL SEGURO

27. Estas funcionalidades de seguridad mitigan la amenaza (A.RED).
28. **COM.1** 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.).
29. **COM.2** El TOE debe permitir que estos canales de comunicación seguros sean iniciados por él mismo o por entidades autorizadas.
30. **COM.3** El producto hará uso de certificados digitales para la autenticación cuando utilice cualquiera de estos protocolos.

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

31. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL, A.SEG).
32. **ACT.1** El producto ofrecerá la posibilidad de consultar la versión actual del *software*, iniciar actualizaciones manualmente y comprobar si existen nuevas actualizaciones disponibles.
33. **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 *software* antes de instalarlas.
34. **ACT.3** La actualización del *software* se permitirá únicamente a usuarios con rol de administrador.
35. **ACT.5** El producto deberá estar empaquetado de forma que, si se elimina, no deje rastro de su instalación (excepto por configuraciones y ficheros de salida o auditoría).
36. **ACT.6** El producto no descargará ni modificará su propio código binario.
37. **ACT.7** El producto solamente utilizará las bibliotecas de terceras partes declaradas por el fabricante.

4.6 CAPACIDAD ANTI-EXPLOTACIÓN

38. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL).
39. **EXP.1** Capacidades anti-explotación. El producto se auto-protegerá cuando se encuentre en ejecución, de tal forma que tenga acceso exclusivo a su zona de memoria asignada.
40. **EXP.2** El producto está configurado por defecto con permisos de ficheros que lo protejan de accesos no autorizados.

4.7 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

41. Estas funcionalidades de seguridad mitigan la amenaza (A.REST). **Podrán ser cubiertas por el producto o por su entorno operacional.**
42. **CRD.1.** En el caso en que el producto almacene credenciales y/o datos sensibles, éstos no deberán almacenarse en claro.
43. **CRD.2.** En el caso en el que el producto utilice sus propias credenciales de acceso, el producto obligará al cambio/establecimiento de credenciales cuando el acceso se realice utilizando credenciales por defecto o el usuario no tenga asignadas credenciales.

4.8 REQUISITOS CRIPTOGRÁFICOS

44. Estas funcionalidades de seguridad mitigan las amenazas (A.RED, A.REST).

45. **CIF.1** El TOE permitirá exclusivamente el empleo de funciones, algoritmos y protocolos que utilicen suites de cifrado que estén incluidas entre las autorizadas para Categoría MEDIA del ENS, de acuerdo a lo establecido en la guía CCN-STIC-807.

46. **CIF.2** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas).

4.8.1. REQUISITOS GESTIÓN DE IDENTIDADES

47. Estas funcionalidades de seguridad mitigan las amenazas (**A.INSUF_ATRB**).

48. **IDM.1** El producto deberá garantizar que cada usuario tiene asociado un único identificador y deberá tener la capacidad de definir la información de identidad y credenciales asociadas a los usuarios de la organización (por ejemplo: nombre, identificador empleado, teléfono, departamento, rol, etc.).

49. **IDM.2** Con respecto a las **credenciales**, el producto deberá:

    a) Definir el **tiempo de vida** de las credenciales, junto con los **estados** de las mismas.

    b) Actualizar el **estado** de las credenciales siempre que haya un cambio que lo requiera.

    c) Permitir consultar el **estado** de las credenciales.

    d) **Revocar** credenciales de usuarios.

    e) Permitir que un servidor de autenticación autorizado actualice las credenciales.

50. **IDM.3.** Las credenciales asociadas a los usuarios de la organización, deben cumplir las siguientes reglas:

    Para credenciales basadas en contraseñas:

    a) La longitud mínima de la contraseña será establecida por el administrador, debiendo soportar contraseñas de 12 caracteres o más.

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

    c) Las reglas de composición de la contraseña que especifiquen el tipo y número de caracteres requeridos, deben poder ser establecidas por el administrador.

    d) El número de últimas contraseñas establecidas por el usuario, que no se pueden reutilizar, será un parámetro a establecer por el administrador.

    Para credenciales no basadas en contraseñas:

    a) La probabilidad de que un atacante pueda descubrir el secreto durante su tiempo de vida, ha de ser menor que 2^{-20}.

51. **IDM.4.** El producto deberá transmitir los datos de identidades y credenciales a otras entidades autorizadas del entorno operacional que lo requieran. La transmisión de estos datos podrá realizarse tras su creación o modificación, de forma periódica, o bajo petición de estos productos.
52. **IDM.5**. La transmisión de los datos indicados en IDM.4 deberá efectuarse a través de un canal seguro tal y como establece COM.1, y con autenticación mutua.

4.9 NOTAS DE APLICACIÓN

53. 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***.
54. 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
ESM	*Enterprise Security Management*
NIAP	*National Information Assurance Partnership*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*
TOE	*Target of Evaluation*