centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo A.7-M: Gestión de Identidades (IM)

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 09:39:11 +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 **Gestión de Identidades (IM, *Identity Management*)** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos y Servicios STIC (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

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.

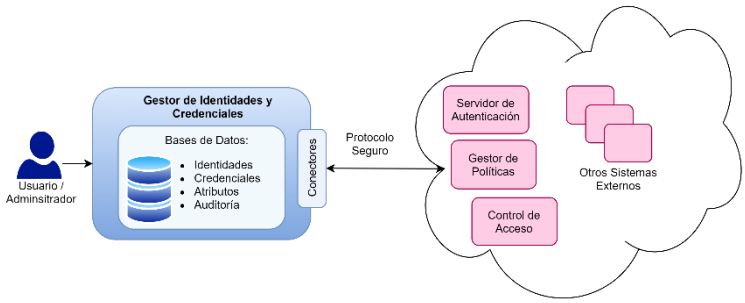

Figura 1 – Caso de Uso Gestor de Identidades y Credenciales con almacenes de datos propios

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.

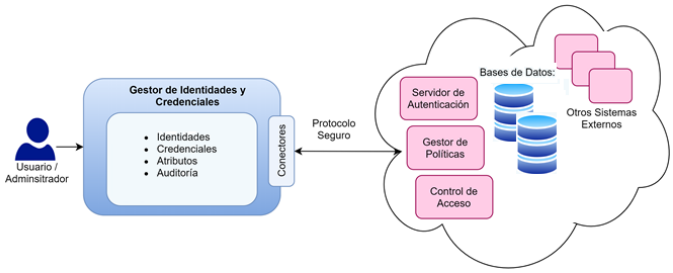

Figura 2 – Caso de Uso Gestor de Identidades y Credenciales sin almacenes de datos propios

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

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.** 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 *Gestión de Identidades* 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

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 CERTIFICACIÓN LINCE

17. 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 ACTIVOS SENSIBLES A PROTEGER

18. 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

19. 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.

3.3 TRAZABILIDAD AMENAZAS/REQUISITOS DE SEGURIDAD

20. 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
ADM.1	X								
ADM2	X								
ADM.3	X								
IAU.1	X							X	
IAU.2									X
IAU.3									X
IAU.4	X								
COM.1		X	X						
COM.2			X						
COM.3			X						
COM.4		X	X						
ACT.1				X					

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

4. REQUISITOS DE SEGURIDAD

21. 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.

22. 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

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

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

25. **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].

26. **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

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

28. **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*].

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

30. **IAU.3** El TOE debe disponer de la capacidad de gestión de las contraseñas:

    a) La contraseña debe de 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.

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

4.3 CANALES SEGURO

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

33. **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*].

34. **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.

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

36. **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

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

38. **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

39. **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].

40. **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.

41. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.

42. **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).

43. **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

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

45. **AUD.1** El producto 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].

46. **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.
47. **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]
48. **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].
49. **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

50. **EXP.1** Cuando el TOE se encuentre en ejecución, este no solicitará la asignación de ninguna dirección explícita de memoria del sistema, ni asignará memoria con permisos simultáneos de escritura y ejecución.
51. **EXP.2** El TOE está configurado por defecto con permisos de ficheros que lo protejan de accesos no autorizados.
52. **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

53. **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 GESTIÓN DE IDENTIDADES

54. **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 *[**selección**:* nombre; identificador empleado; teléfono; departamento; rol; *[**asignación**: otros parámetros*].

55. **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.

56. **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.

57. **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 *[**selección**: tras su creación o modificación; de forma periódica; bajo petición de estos productos*].

58. **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.

4.10 NOTAS DE APLICACIÓN

59. 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***.

60. 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*

PUBLICACIONES DE DEFENSA

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