Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo A.6-M: Gestión de acceso privilegiado (PAM)

Noviembre de 2022

MINISTERIO DE DEFENSA

cpage.mpr.gob.es

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 09:38:42 +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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia de ***Gestión de acceso privilegiado (PAM, Privileged Access 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 a 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 acceso privilegiado (PAM)** 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. Las cuentas privilegiadas son cuentas que proporcionan un acceso con alto nivel de permisos a los recursos TI de la organización. Estas cuentas pueden corresponder a una persona física o no, como las cuentas que utilizan las aplicaciones para ejecutar servicios o comandos que requieren permisos especiales, aunque normalmente existen para permitir a los profesionales TI gestionar aplicaciones, software o recursos hardware.
7. Las cuentas privilegiadas son, por lo tanto, las cuentas más críticas y potentes dentro de la infraestructura TI y son, habitualmente, uno de los principales objetivos de los ciberataques que pretenden obtener acceso a la información y a los recursos de la organización.
8. La protección y el control de los accesos a estas cuentas privilegiadas que administran activos y datos críticos, junto con la necesidad de seguir dando a usuarios, aplicaciones y administradores la flexibilidad que necesitan para realizar sus tareas diarias, es una misión compleja que puede simplificarse a través del uso los productos de Gestión de cuentas privilegiadas, también llamados **productos PAM** (*Privileged Access Management*).
9. Todos los productos de la familia PAM persiguen, por lo tanto, el mismo objetivo: prevenir un uso indebido de cuentas privilegiadas en los sistemas, dispositivos y aplicaciones TI de la organización y permitir administrar y monitorizar el uso de estas cuentas.
10. En el ámbito comercial existe una gran variedad de productos que difieren en las funcionalidades y en las características de seguridad que ofrecen. En este contexto, a continuación, se indican las características más comunes que puede proporcionar un producto PAM:
    a) **Almacén seguro de credenciales (*Vault*)**, que preserva la confidencialidad e integridad de las credenciales asociadas a las cuentas privilegiadas, y las protege de accesos no autorizados.
    b) **Control de acceso** a los recursos TI gestionados a través de las cuentas privilegiadas, basado en las políticas establecidas por la organización y/o configuradas por el administrador PAM.
    c) **Implementación automática (*Enforcement*) de la política de contraseñas**, permitiendo generar, actualizar y mantener de forma automática, las contraseñas y otras credenciales de las cuentas privilegiadas.
    d) **Descubrimiento automático de cuentas privilegiadas** existentes en los sistemas, dispositivos o aplicaciones de la organización, y que pueden no haber sido declaradas.
    e) **Seguridad basada en roles** para grupos de usuarios que requieren el mismo nivel de acceso.

f) **Registro y monitorización de sesiones en tiempo real**, permitiendo registrar y supervisar la actividad de las sesiones de cuentas privilegiadas, incluyendo las acciones y comandos ejecutados.

2.2 CASOS DE USO

11. Aunque, como ya se ha indicado anteriormente, los productos PAM realizan implementaciones muy distintas, a continuación, se indican las funciones más comunes que componen este tipo de productos.

- **Gestor de Conexión o *Broker***, que recibe la solicitud de conexión de un usuario, y la envía a un Gestor Central o Master para su evaluación. En caso de que el Master acepte la solicitud, el *broker* establecerá la conexión con el recurso TI en nombre del usuario, sin necesidad de que este conozca las credenciales privilegiadas.
- **Gestor Central o Master**, que recibe, a través del *broker*, las solicitudes de conexión de los usuarios y las evalúa de acuerdo con la política de seguridad vigente, para rechazar o aceptar la conexión.
- **Gestor de Políticas**, que procesa las directivas procedentes de las políticas de seguridad corporativas y aplicables a las cuentas privilegiadas que gestiona. En algunos casos tiene capacidad de "*Policy Enforcement*", aplicando de forma automática políticas de rotación y actualización de contraseñas sobre los recursos TI.
- **Gestor de Auditoría**, que permite no solo generar registros de auditoría con los eventos de seguridad relevantes del sistema, sino que también monitoriza y "graba" las actividades que ocurren durante la sesión privilegiada, para proporcionar posteriormente una reproducción de la sesión a los administradores autorizados. Los registros generados pueden almacenarse en un almacén de auditoría propio, o bien enviarse a un servidor de auditoría externo.
- **Gestor de Configuración**, que permite a los administradores configurar, administrar y monitorizar las políticas de seguridad, cuentas privilegiadas y, en general, todas las funciones de gestión y administración del producto. El acceso local y/o remoto a este gestor de configuración se realiza, en algunos casos, a través de interfaces de gestión.
- **Gestor de Descubrimiento**, que permite descubrir de forma automática nuevas cuentas privilegiadas en los recursos TI gestionados.
- ***Broker* de Comandos**, similar al *Broker* de Conexión, permite realizar un control de acceso a los recursos TI no solo a nivel de sesión, sino a nivel de comando privilegiado. Esto permite que los usuarios puedan ejecutar ciertos comandos y realizar tareas privilegiadas con su propia cuenta personal, sin necesidad de elevar sus privilegios (*least privilege*).

- **Gestor de Aplicaciones**, que permite facilitar el acceso privilegiado que algunas aplicaciones software requieren a ciertos recursos TI, sin necesidad de introducir las credenciales privilegiadas en el código de la aplicación o script.
- **Clientes**, software específico para establecer las conexiones de administración remotas, y las conexiones de los usuarios privilegiados desde los *endpoints*.
- **Almacén seguro de credenciales (*Vault*).** Algunos productos PAM proporcionan un almacenamiento seguro para las credenciales privilegiadas de los sistemas TI que gestionan. Estas credenciales no se deberán nunca almacenar en texto claro, sino que irán protegidas con algún mecanismo criptográfico.
- **Almacén seguro de registros de auditoría.** Algunos productos PAM proporcionan un almacenamiento seguro para los registros de auditoría, tanto los correspondientes a los eventos de seguridad del propio sistema, como los registros o "grabaciones" de las acciones realizadas en las sesiones establecidas por los usuarios privilegiados.

12. Cada producto PAM puede proporcionar una o varias de estas funciones, integradas en uno o varios componentes lógicos. Algunos productos integran todos sus componentes lógicos dentro de un *appliance* físico, mientras que otros, proporcionan varios paquetes software distribuidos en dispositivos hardware estándar.
13. La siguiente figura recoge un ejemplo de implementación de este tipo de productos.

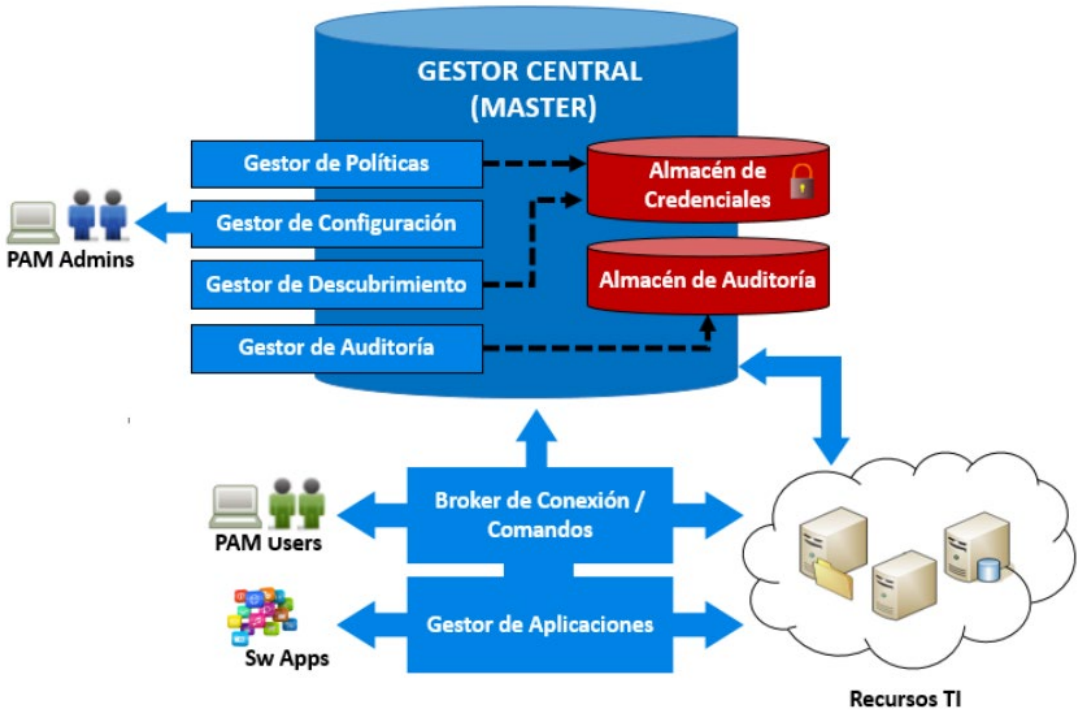

Figura 1 – Ejemplo de implementación PAM

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

14. En este apartado se indican algunas condiciones generales y específicas que se requieren en el entorno operativo en el que se vaya a desplegar el producto, para garantizar su seguridad:

    - **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 *gestion de acceso privilegiado* 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

15. Este tipo de productos se pueden presentar tanto en formato de paquete *software*, a instalar sobre los correspondientes equipos *Hardware* compatibles y previamente bastionados (*hardened*), o bien en formato Equipo dedicado o *Appliance* (*hardware* provisto de firmware dedicado) con las funcionalidades necesarias para cumplir su finalidad, y acotadas al servicio específico que presente.

2.5 CERTIFICACIÓN LINCE

16. Para que un producto de esta familia pueda ser incluido en el CPSTIC como producto cualificado 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

17. 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

18. 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

19. 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.FUN	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									
IAU.5										X
COM.1		X	X							
COM.2			X							
COM.3			X							
COM.4		X	X							

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.INT	A.PSC	A.FUN	A.NOAUTUSR	A.CRE
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.1						X				
EXP.2						X				
EXP.3						X				
PSC.1							X			
CIF.1		X	X							
CIF.2		X	X							
PAM.1	X	X	X					X		
PAM.2					X					
PAM.3					X					
PAM.4	X	X			X					
PAM.5		X								
PAM.6	X	X								
PAM.7									X	
PAM.8									X	
PAM.9	X							X		
PAM.10	X								X	

4. REQUISITOS DE SEGURIDAD

20. 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.

21. 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

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

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

24. **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*].

25. **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

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

27. **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*].

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

29. **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.

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

31. **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 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 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*].

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 CAPACIDAD 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 PAM

54. **PAM.1** Si el producto implementa la funcionalidad de *Gestor de Conexión*, este debe poder establecer, en nombre del usuario, sesiones privilegiadas con el recurso IT. Las credenciales de acceso privilegiado a dicho recurso serán transparentes al usuario.
55. **PAM.2** Si el producto implementa la funcionalidad de *Almacén seguro de registros de auditoría*, este debe monitorizar y registrar las actividades realizadas durante el otorgamiento de acceso de cuentas privilegiadas y las actividades realizadas por el usuario durante las sesiones con cuentas privilegiadas.
56. **PAM.3.** Si los registros de auditoría de actividad son almacenados de forma local (funcionalidad de *Gestor de Auditoría*), estos deben ser protegidos frente a accesos no autorizados.
57. **PAM.4.** Si los registros de auditoría de actividad son almacenados de forma remota (funcionalidad de *Gestor de Auditoría*), en un servidor externo de auditoría, los registros deben ser enviados de acuerdo a lo indicado en COM.1.
58. **PAM.5.** Si el producto implementa la funcionalidad de Vault, este debe proteger criptológicamente el almacenamiento de las credenciales privilegiadas, según CIF.1.
59. **PAM.6.** Si el producto implementa la funcionalidad de *Gestor de Configuración*, este debe poder definir y transmitir de forma segura datos de identidades y credenciales a otras soluciones de gestión de sesiones y credenciales.
60. **PAM.7.** Si el producto implementa la funcionalidad de Gestor de Configuración. El producto debe poder definir políticas de contraseñas para garantizar que las cuentas privilegiadas utilizan contraseñas seguras para acceder a los recursos IT gestionados.
61. **PAM.8.** Si el producto implementa la funcionalidad de *Gestor de Políticas*, este debe actualizar periódicamente las contraseñas de acceso a los recursos IT de forma transparente al usuario final.
62. **PAM.9.** Si el producto implementa la funcionalidad de *Gestor de Políticas*, este debe permitir establecer políticas de control de acceso que permitan asociar usuarios con los recursos o servicios IT a los que tiene acceso.
63. **PAM.10.** Si el producto implementa la funcionalidad de *Gestor de Descubrimiento*, este debe incluir mecanismos para realizar el descubrimiento de cuentas privilegiadas en el entorno en el que opera.

4.10 NOTAS DE APLICACIÓN

64. 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***.

65. 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