centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

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

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 10:20:05 +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 de ***Gestión de acceso privilegiado (PAM, Privileged Access 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 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.

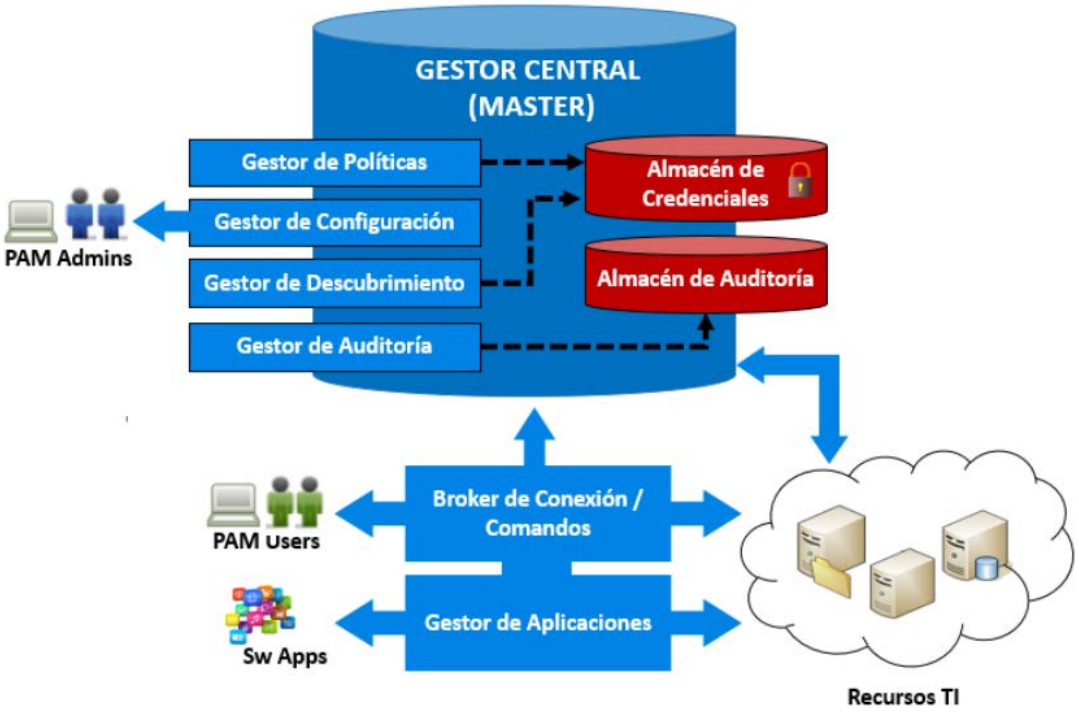

Figura 1 – Ejemplo de implementación PAM.

2.3 ENTORNO DE USO

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:

    a) **Protección física:** las plataformas hardware asociadas al producto, deberán estar físicamente protegidas en su entorno operativo y no sujetas a ataques físicos que comprometan y/o interfieran con los dispositivos. El entorno deberá, por lo tanto, proporcionar la seguridad física acorde con el valor de los datos que protege el producto.

    b) **Administración confiable:** los usuarios 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.

    c) **Plataforma confiable y bastionada:** en el caso de productos *software*, este ejecutará sobre una plataforma confiable y bastionada, incluyendo el sistema operativo o cualquier entorno de ejecución sobre el que se utilice.

    d) **Entidades de terceros confiables:** en el caso de que el producto intercambie información de identidades o atributos con entidades de terceros, estas deberán ser de confianza.

e) **Actualizaciones periódicas:** El producto será puesto al día conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.

f) **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:

- Servidor de credenciales (p.e Directorio Activo).
- Servidor de Auditoría.
- Fuente de tiempo fiable (*reliable timestamp*).
- Servidor de políticas corporativas.
- Servidor de identidades.
- Primitivas criptográficas

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 RECURSOS QUE ES NECESARIO PROTEGER

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

    a) **Datos críticos almacenados:**

    - Credenciales que permiten el acceso privilegiado a los recursos TI de la organización, gestionados por el producto PAM.
    - Datos de configuración del producto.
    - Datos de auditoría relativos a las acciones que el usuario haya llevado a cabo durante la sesión privilegiada, o a las acciones realizadas por los administradores sobre la configuración del producto.
    - Claves y otros parámetros críticos de seguridad (*Critical Security Parameters, CSPs*) utilizados para las funciones criptográficas.

    b) **Datos críticos intercambiados entre los distintos componentes del producto, o entre el producto y otras entidades o recursos TI autorizados:**

    - Datos de administración, configuración y gestión del producto intercambiados a través de las interfaces de gestión.
    - Datos de identidad y credenciales de acceso privilegiado a los recursos TI gestionados.
    - Datos de autenticación intercambiados con servidores externos de autenticación (*AAA servers*).
    - Datos de auditoría intercambiados con servidores externos de auditoría (*Audit servers*).

    c) **Recursos TI de la organización a los que los usuarios pueden acceder, a través del producto, con cuentas privilegiadas.**

3.2 AMENAZAS

18. 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.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

19. A continuación, se recogen los requisitos que deben cumplir los productos de Gestión de cuentas privilegiadas (PAM).

4.1 ADMINISTRACIÓN CONFIABLE

20. Estas funcionalidades de seguridad mitigan la amenaza (A.SEG). **Podrán ser cubiertas por el producto o por su entorno operacional.**
21. **ADM.1** El producto debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.
22. **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.
23. **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

24. Estas funcionalidades de seguridad mitigan la amenaza (A.REST, A.SEG). **Podrán ser cubiertas por el producto o por su entorno operacional.**
25. **IAU.1.** El producto deberá identificar y autenticar a cada usuario antes de otorgar acceso.
26. **IAU.2.** El producto deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
27. **IAU.3.** El producto deberá proteger de lectura y modificación no autorizada las credenciales de autenticación.
28. **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 [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “]
29. **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

30. Estas funcionalidades de seguridad mitigan la amenaza (A.NODET).
31. **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
    e) Generación, importación y borrado de claves criptográficas.
32. **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).
33. **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.
34. **AUD.4**. El producto debe ser capaz de almacenar la información de auditoría generada en sí mismo o en una entidad externa.
35. **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

36. Estas funcionalidades de seguridad mitigan la amenaza (A.RED).
37. **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.).
38. **COM.2** El TOE debe permitir que estos canales de comunicación seguros sean iniciados por él mismo o por entidades autorizadas.
39. **COM.3** El producto hará uso de certificados digitales para la autenticación cuando utilice cualquiera de estos protocolos.

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

40. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL, A.SEG).

41. **ACT.1** El producto ofrecerá la posibilidad de consultar la versión actual del *software*, iniciar actualizaciones manualmente y comprobar si existen nuevas actualizaciones disponibles.
42. **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.
43. **ACT.3** La actualización del *software* se permitirá únicamente a usuarios con rol de administrador.
44. **ACT.5** En el caso de tratarse de una aplicación *software*, **e**l 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).
45. **ACT.6** En el caso de tratarse de una aplicación *software*, el producto no descargará ni modificará su propio código binario.
46. **ACT.7** En el caso de tratarse de una aplicación *software,* el producto solamente utilizará las bibliotecas de terceras partes declaradas por el fabricante.

4.6 CAPACIDAD ANTI-EXPLOTACIÓN

47. Estas funcionalidades de seguridad mitigan la amenaza (A.LOCAL) y aplicarán en el caso de tratarse de una aplicación *software*.
48. **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.
49. **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

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

53. Estas funcionalidades de seguridad mitigan las amenazas (A.RED, A.REST). **Podrán ser cubiertas por el producto o por su entorno operacional.**

54. **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.

55. **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 PAM

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

2. **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.

3. **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.

4. **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.

5. **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.

   PAM.5. Si el producto implementa la funcionalidad de *Vault*, este debe proteger criptológicamente el almacenamiento de las credenciales privilegiadas, según CIF.1.

6. **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.

7. **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.

8. **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.

9. **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.

10. **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.

4.9 NOTAS DE APLICACIÓN

11. 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***.
12. 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*