centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

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

Julio 2019

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

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
2019.07.19 10:01:15 +02'00'

NIPO: 083-19-053-9.

Fecha de Edición: julio de 2019

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 Mangement*)** 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). 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 mas 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 del potencial uso indebido de cuentas privilegiadas en los sistemas, dispositivos y aplicaciones TI de la organización, permitiendo administrar y monitorizar el uso de estas cuentas por parte de los usuarios. Sin embargo, la implementación que realizan los productos de esta familia, y las características de seguridad que ofrecen, difieren mucho de un producto a otro.

10. 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 del 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.

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.

12. La siguiente figura recoge un ejemplo de implementación de este tipo de productos.

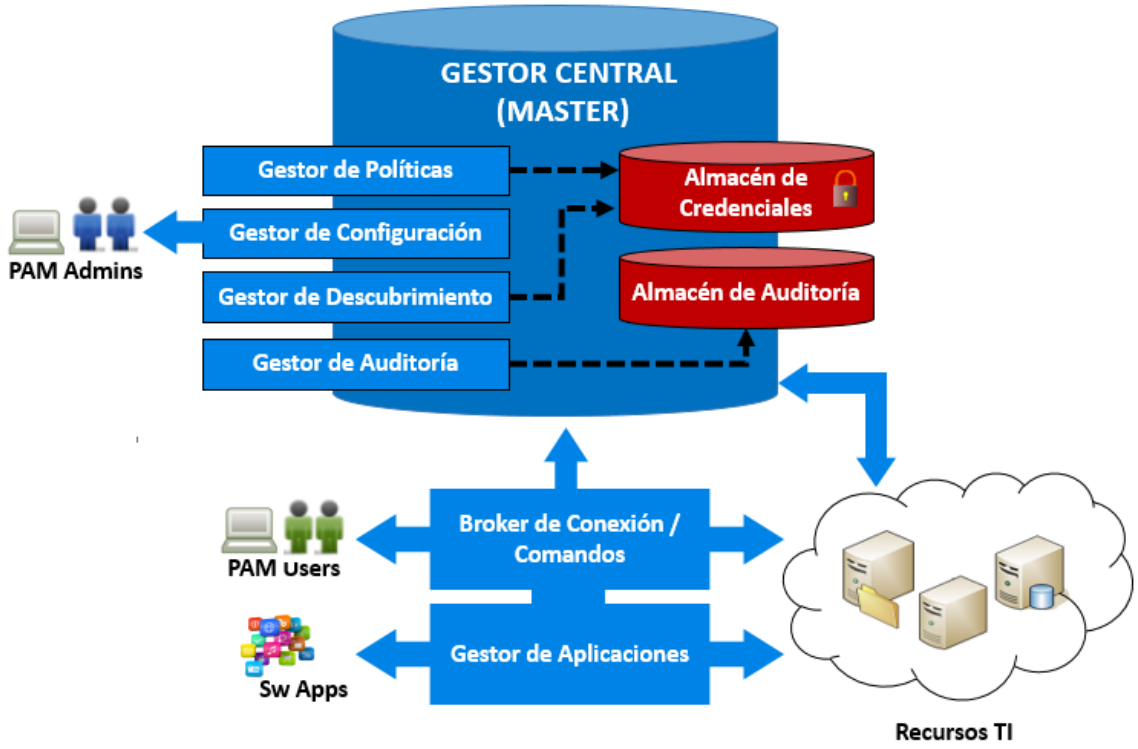

Figura 1. Ejemplo de implementación PAM.

2.3 ENTORNO DE USO

13. 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 fortificada (*hardened*) y compatible**: en el caso de productos software, las plataformas hardware en las que se instale el producto deberán ser perfectamente compatibles, estar adecuadamente reforzadas y

no deben haber sido comprometidas previamente a la instalación del producto.

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 confiables.

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

14. Este tipo de productos se pueden presentar tanto en formato de paquete Software, a instalar sobre los correspondientes equipos Hardware compatibles y previamente fortificados (*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 presten.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

15. El estándar *Common Criteria (CC)* proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TIC (Tecnologías de la Información y de las Comunicaciones).
16. En el ámbito de CC se elaboran unos perfiles de seguridad (*Protection Profiles*) que definen, para un dominio o categoría de productos, un conjunto de objetivos y requisitos de seguridad, tanto funcionales como de evaluación, independientes de la implantación.
17. Los productos dentro de esta familia deberán cumplir con los RFS reflejados en el apartado 4, y con los SFR (*Security Functional Requirements*) que se especifican en alguno de los siguientes perfiles de protección, certificados de acuerdo a la norma *Common Criteria:*

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Enterprise Security Management - Identity and Credential Management [1]	*2.1*	*21/11/2013*	*NIAP*
Protection Profile for Enterprise Security Management - Policy Management [2]	*2.1*	*21/11/2013*	*NIAP*
Protection Profile for Enterprise Security Management-Access Control [3]	*2.1*	*12/11/2013*	*NIAP*

18. En caso de que el producto no esté certificado contra ninguno de los perfiles anteriores, debe disponer de una declaración de seguridad (*Security Target*) certificada con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**. La declaración de seguridad debe implementar los SFR (*Security Functional Requirements*) apropiados para satisfacer, al menos, los Objetivos de Seguridad que se indican en el apartado 4.1.

[1] https://www.niap-ccevs.org/MMO/PP/pp_esm_icm_v2.1.pdf
[2] https://www.niap-ccevs.org/MMO/PP/pp_esm_pm_v2.1.pdf
[3] https://www.niap-ccevs.org/MMO/PP/pp_esm_ac_v2.1.pdf

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

19. Los recursos que es necesario proteger mediante el uso 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

21. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente serían:

    a) **Compromiso de los datos críticos:** un usuario malintencionado puede intentar acceder a los datos críticos almacenados en el producto o transmitidos entre las distintas partes del mismo o con otras entidades externas, para modificarlos, destruirlos u obtener credenciales que podría reproducir para hacerse pasar por otro usuario autorizado.

    b) **Compromiso de los registros de auditoría:** un usuario o proceso malintencionado puede acceder de forma no autorizada a los registros de auditoría, y provocar la pérdida o la modificación de los mismos, o intentar enmascarar sus acciones, causando con ello que los datos de auditoría se registren incorrectamente o que nunca se registren.

    c) **Acceso no autorizado:** un usuario malintencionado podría saltarse los mecanismos de identificación, autenticación o autorización del producto para obtener acceso ilícito a sus funciones o recursos.

    d) **Errores de administración:** un administrador podría instalar o configurar el producto incorrectamente, aunque de forma no intencionada, provocando la falta de efectividad de los mecanismos de seguridad.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

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

4.1 PERFIL DE PROTECCIÓN COMMON CRITERIA

23. **REQ. 1**. Los productos deberán estar certificados con alguno de los siguientes perfiles de protección de acuerdo a la norma Common Criteria:

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Enterprise Security Management - Identity and Credential Management [4]	*2.1*	*21/11/2013*	*NIAP*
Protection Profile for Enterprise Security Management - Policy Management [5]	*2.1*	*21/11/2013*	*NIAP*
Protection Profile for Enterprise Security Management-Access Control [6]	*2.1*	*12/11/2013*	*NIAP*

24.

Tabla 1. Perfiles de Protección.

25. **REQ. 2**. En caso de que el producto no esté certificado contra ninguno de los perfiles anteriores, debe disponer de una declaración de seguridad (*Security Target*) certificada con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**. La declaración de seguridad debe implementar los SFR (*Security Functional Requirements*) apropiados para satisfacer, al menos, los Objetivos de Seguridad que se recogen en la siguiente tabla:

[4] https://www.niap-ccevs.org/MMO/PP/pp_esm_icm_v2.1.pdf
[5] https://www.niap-ccevs.org/MMO/PP/pp_esm_pm_v2.1.pdf
[6] https://www.niap-ccevs.org/MMO/PP/pp_esm_ac_v2.1.pdf

OBJETIVO	DESCRIPCIÓN
[PROTECCIÓN DE LAS CREDENCIALES]	El producto no debe almacenar los datos de credenciales en texto claro y debe protegerlos de accesos no autorizados.
[CONTROL DE ACCESO] IDENTIFICACIÓN Y AUTENTICACIÓN	El producto debe identificar de forma única a los usuarios, y autenticarlos antes de permitirles acceso las funciones y datos del producto.
[CONTROL DE ACCESO] CONSENTIMIENTO	El producto debe permitir informar a los usuarios sobre el uso no autorizado de la sesión, antes de su establecimiento.
[CONTROL DE ACCESO] CONTROL DE SESIONES	El producto debe implementar mecanismos que permitan suspender o denegar el establecimiento de una sesión.
[GESTIÓN DE LA SEGURIDAD] FUNCIONALIDAD	El producto debe proporcionar un conjunto de funciones que permitan el control de sus funciones y datos, asegurándose de que solo los usuarios con los privilegios adecuados (administradores) puedan ejercer dicho control.
[GESTIÓN DE LA SEGURIDAD] PERMISOS	El producto debe permitir la definición de perfiles de administración (*roles*), y la asignación de distintas funciones de gestión a cada perfil (*separation of duties*).
[PROTECCIÓN DE LAS COMUNICACIONES]	El producto debe proteger la confidencialidad y la integridad de los datos transmitidos entre los componentes del producto, y entre el producto y los administradores u otras entidades IT externas.
[AUDITORÍA] REGISTRO DE EVENTOS	El producto debe tener la capacidad de detectar los eventos relevantes de seguridad, y registrarlos adecuadamente en los registros de auditoría.
[AUDITORÍA] PROTECCIÓN DE LOS REGISTROS	El producto debe proteger los registros de auditoría almacenados o trasmitidos, de accesos no autorizados.

Tabla 2. Objetivos de Seguridad.

4.2 AUDITORÍA Y MONITORIZACIÓN

26. **REQ. 3**. El producto debe monitorizar y registrar las actividades realizadas por los usuarios durante las sesiones con cuentas privilegiadas.
27. **REQ. 4**. En caso de que estos registros de auditoría de actividades se almacenen de forma local, deberán ser protegidos de accesos no autorizados.
28. **REQ. 5**. En caso de que estos registros de auditoría de actividades se almacenen de forma remota en un servidor de auditoría externo, deberán ser enviados mediante un protocolo seguro (IPsec, TLS 1.2 o superior, SSH, etc).

4.3 MÍNIMO PRIVILEGIO

29. **REQ. 6**. El producto debe tener la capacidad de establecer las sesiones privilegiadas con el recurso TI gestionado, en nombre del usuario, de forma que este no conozca en ningún momento, las credenciales privilegiadas de acceso al recurso.

4.4 SOPORTE CRIPTOGRÁFICO

30. **REQ. 7**. En caso de que el producto utilice algoritmos y funciones criptográficas, debe soportar el uso de aquellas aceptadas para nivel Alto del ENS según la guía CCN-STIC-807, así como proporcionar capacidades de configuración que permitan obligar al uso de estos algoritmos exclusivamente.
31. **REQ. 8.** El producto debe soportar el uso de longitudes de clave que proporcionen una fortaleza equivalente a 128 bits o superior.

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
EPP	*Endpoint Protection Platform*
NIAP	*National Information Assurance Partnership*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*