Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo A.4M: Servidores de Autenticación

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

CCN 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 09:36:58 +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 de Servidores de Autenticación 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 **Servidores de Autenticación**, 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 esta familia están orientados a verificar la identidad de un usuario o dispositivo, en función de uno o varios factores, dentro de una arquitectura de red protegida. Estos productos suelen situarse justo delante de los servicios de una organización para asegurar que son utilizados únicamente por aquellas identidades autorizadas, de acuerdo a la política de seguridad de la organización.

7. En este contexto, las funciones básicas de seguridad que proporcionan esta familia de productos son las siguientes:

    - **Identificación y autenticación de usuarios**. Permiten la aplicación de una política de seguridad centralizada y común para el control de acceso a servicios o sistemas de diferente naturaleza interconectados con el producto, además de proporcionar mayor transparencia al usuario en el proceso de autenticación a los servicios o sistemas a los que el producto le habilite el acceso, en función de sus permisos.

    - **Autenticación multifactor**. Permiten utilizar conjuntamente diferentes formas de autenticación (p.ej. contraseña conocida por el usuario y código de seguridad enviado a un dispositivo móvil que posee el usuario) para confirmar con mayor fiabilidad la identidad de un usuario.

    - **Ruptura del protocolo de autenticación**. Todos los procesos de autenticación requeridos por los servicios utilizados en la organización pasan por el servidor de autenticación, que está diseñado e implementado de forma segura para evitar ataques frente a los que los servicios que protegen pueden ser vulnerables.

8. Los productos incluidos en esta familia pueden ofrecer otras funcionalidades complementarias (p.ej. control de acceso a red) no contempladas específicamente en este documento.

2.2 CASOS DE USO

9. Para esta familia de productos tan sólo se contempla un caso de uso, en el que el servidor de autenticación hace de medio de identificación y autenticación para el acceso a los servicios de la organización. Existe la posibilidad de que la forma de autenticación varíe (multifactor, credenciales, biometría, etc.) pero la implementación y funcionalidad del producto sigue siendo la misma.

2.2.1. CASO DE USO 1 – PASARELA DE IDENTIFICACIÓN Y AUTENTICACIÓN A LOS SERVICIOS

10. El servidor de autenticación se sitúa entre los servicios que ofrece una red y los usuarios de esta, actuando como una frontera entre ambos. Una vez se identifica y

autoriza un acceso, el servidor de autenticación se limita a mantener la sesión activa y delega el control de acceso a los servicios que se encuentran tras él.

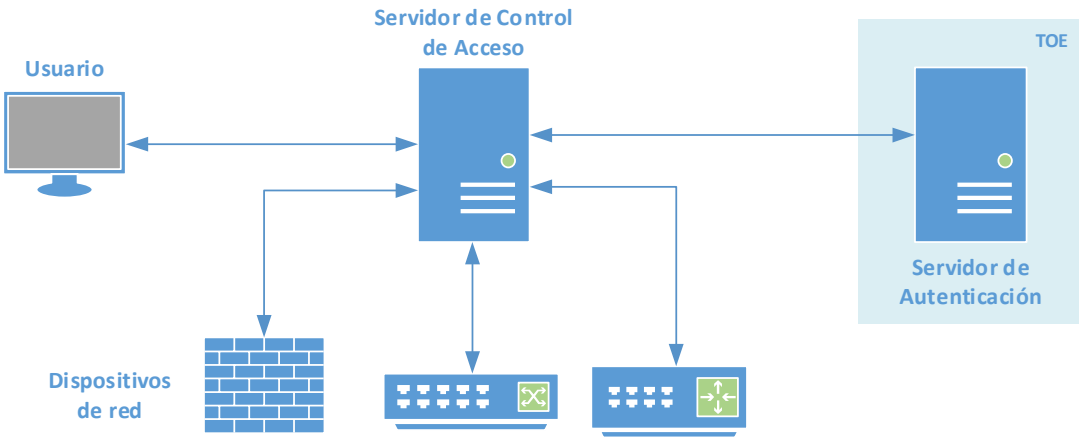

Figura 1 - Ejemplo de Caso de Uso 1: Pasarela de autenticación a los servicios

11. El servidor de control de acceso es opcional y su funcionalidad podría ser implementada por el servidor de autenticación. En cualquier caso, dicha funcionalidad deberá ser cualificada de forma independiente (ver *Anexo A1 Dispositivos de Control de Acceso a red*).

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

12. Por lo general, estos dispositivos se utilizan en grandes o medianas empresas y en redes del sector público, junto con otras medidas de seguridad complementarias, formando parte de una arquitectura de defensa en profundidad que busca proteger el entorno de comunicación.
13. Para la utilización en condiciones óptimas de seguridad de estos productos, es necesaria su integración en un entorno operacional que cumpla las siguientes condiciones:

    - **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 *autenticación* a red 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.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

14. Este tipo de productos se presenta en formato de *appliance* dedicado, que proporciona la funcionalidad que deberá tener la capacidad de soportar y manejar multitud de conexiones simultáneas, ya que actúa como punto intermedio entre los usuarios y los servicios.
15. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2.1, estas quedan fuera del alcance analizado, y deberán ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

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 deben protegerse mediante el uso de estos 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, atendiendo al caso de uso expuesto en la sección 2.1, 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.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.FUN Fallo de las funcionalidades de seguridad:** Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad declaradas del producto y podría acceder, cambiar o modificar información, funcionalidades de seguridad o tráfico de red en el producto.
- **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.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								
COM.1		X	X						
COM.2			X						
COM.3			X						
COM.4		X	X						
ACT.1				X					
ACT.2				X					
ACT.3				X					
AUD.1					X				
AUD.2					X				
AUD.3					X				

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.PSC	A.FUN	A.NOAUTUSR	A.CRE
AUD.4					X				
AUD.5					X				
PSC.1						X			
PRO.1									
CIF.1		X	X						
SRVAUT.1			X						
SRVAUT.2			X						
SRVAUT.3	X							X	X

4. REQUISITOS DE SEGURIDAD

20. A continuación, se recogen los requisitos 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.
- Configuración del secreto compartido RADIUS.
- [**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.

4.3 CANALES SEGUROS

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

32. **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*].

33. **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.

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

35. **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

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

37. **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

38. **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].

39. **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.

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

4.6 AUDITORÍA

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

42. **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].

43. **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.

44. **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]
45. **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].
46. **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 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

47. **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**.

4.8 PROTECCIÓN DEL PRODUCTO Y SUS SERVICIOS

48. **PRO.1** El TOE deberá ser capaz de realizar un test durante el arranque o encendido del producto, [**selección***: periódicamente durante la operación normal del producto; a petición de un usuario autorizado; ninguna*] para verificar la integridad del software/firmware, [***selección**: el correcto funcionamiento de los mecanismos criptográficos; [**asignación**: otros]; ninguno*].

4.9 REQUISITOS SERVIDOR DE AUTENTICACIÓN

49. **SRVAUT.1** El TOE deberá implementar los protocolos RADIUS (RFC 2865, RFC 2869) con EAP-TLS (RFC 5216) para poder gestionar solicitudes de autenticación de otro componente del entorno (Servidor de acceso a red).
50. **SRVAUT.2** El TOE deberá verificar la corrección e integridad de los paquetes en los que se incluyen las solicitudes de autenticación de los usuarios o entidades finales. Para ello deberá implementar el protocolo RADIUS (RFC 2865, RFC 2869).
51. **SRVAUT.3** El TOE deberá de autenticar identidades basándose en las credenciales que recibe. El producto podrá tomar diferentes resultados de autenticación basándose en información contextual [***selección**: fecha y hora; tipo de credencial utilizado; [**asignación**: otros atributos]*].

5. ABREVIATURAS

CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
ENS	Esquema Nacional de Seguridad
RFS	Requisitos Fundamentales de Seguridad
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