Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo D.9A-M: Herramientas de voz por IP (VVoIP)

Septiembre de 2023

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
Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2023

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
2023.10.03 16:51:59 +02'00'

NIPO: 083-23-071-5
Fecha de Edición septiembre de 2023

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 **Herramientas de voz y vídeo por IP (VVoIP)** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos y Servicios STIC (CPSTIC), publicado por el CCN.
2. Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia debe implementar para un determinado caso de uso, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza y considerarse objetivamente cualificado, desde el punto de vista de la seguridad, para ser empleado en los sistemas de información del sector público para los que sea de aplicación el **Esquema Nacional de Seguridad (ENS)**. 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 **Herramientas de voz y Vídeo por IP (VVoIP)** 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. Se considera Herramienta de comunicaciones VoIP/VVoIP a todo producto que permita a dos o más dispositivos, establecer comunicaciones seguras de Voz (VoIP) o Voz y Vídeo (VVoIP) a través de conexiones de datos basadas en redes IP.
7. Los componentes que integran este tipo de productos son de dos tipos:
    a) **VVoIP endpoint,** que puede consistir en un dispositivo hardware dedicado con capacidad VVoIP, o puede tratarse de una aplicación VVoIP que se ejecuta en un dispositivo hardware de propósito general, como un smartphone, tablet o PC.
    b) **Servidor de control de llamadas (SCL),** que puede consistir en un *appliance* dedicado con un firmware no modificable, o puede tratarse de un servidor de propósito general que proporciona la funcionalidad de control de llamadas.
8. El VVoIP endpoint puede actuar como un cliente que se comunica con un servidor de control de llamadas, o puede actuar como su propio servidor de control de llamadas cuando se implementa una arquitectura extremo a extremo (P2P). El VVoIP endpoint debe ser capaz de: descargar de forma segura sus ficheros de actualización de firmware/software desde un servidor interno de la organización (el SCL u otro), establecer una comunicación segura para el control de llamada con el servidor de control de llamadas, y transmitir de forma segura voz/vídeo a otros dispositivos.
9. Para la viabilidad de las comunicaciones VVoIP, estos productos deben proporcionar dos funciones básicas:
    a) Control de llamadas (*Call Control Processing*): señalización para el establecimiento, procesamiento y finalización de las llamadas VVoIP.
    b) Transmisión de los datos de voz/vídeo (*Streaming media*).
10. Generalmente la función de control de llamadas la proporciona un Servidor de control de llamadas (SCL), comúnmente llamado ESC (*Entrerprise Session Controller*) o *Call-Processing Server*.

    La función principal del SCL es el establecimiento, procesamiento y finalización de las llamadas VVoIP. Para ello utiliza protocolos de procesado de llamadas (*Call processing protocols*), como H.323 o SIP. El protocolo más extendido es SIP (*Session Initiation Protocol*) por lo que, en muchos casos, este servidor es también referido como ***SIP Server***. Es también misión del SCL proteger esta señalización con un protocolo seguro que proporcione autenticación y cifrado, por ejemplo, TLS (*Transport Layer Security*).

    Dentro de las capacidades de control de llamadas deberá llevarse a cabo el registro de los detalles de cada llamada (CDRs, *Call Details Records*).

El SCL también se comunica con otra serie de servicios que proporcionan otros componentes de la infraestructura de la organización, como servicios de buzón de voz, conferencia, NTP (*Network Time Protocol*), DNS (*Domain Name System*) y en muchos casos, almacena las actualizaciones de software/ firmware para su distribución a los VVoIP endpoints.

11. Respecto a la transmisión de voz/vídeo (*streaming media*), generalmente se lleva a cabo directamente entre los **VVoIP endpoints**, aunque dependiendo de la arquitectura del producto, el SCL también puede actuar como intermediario redireccionando esta comunicación entre los VVoIP endpoints.

    Es también misión del VVoIP endpoint, proteger estos datos con un protocolo seguro que proporcione autenticación y cifrado, por ejemplo, SRTP (*Secure Real-time Transport Protocol*).

2.2 CASOS DE USO

12. Dada la naturaleza y el objetivo de este tipo de productos, se contemplan dos casos de uso para esta familia, tal y como se indica a continuación.

2.2.1. CASO DE USO 1 – ARQUITECTURA CLIENTE-SERVIDOR SCL

13. El VVoIP endpoint es un cliente que interactúa con un Servidor de control de llamadas (SCL), encargado de establecer, procesar y finalizar las llamadas entre los VVoIP endpoints utilizando para ello un protocolo de control de llamadas (SIP o H.323).

14. En este caso de uso, es el servidor de control de llamadas (SCL) el encargado de las funciones de auditoría del sistema, incluido el registro de los detalles de las llamadas o CDRs (*Call Details Records*).

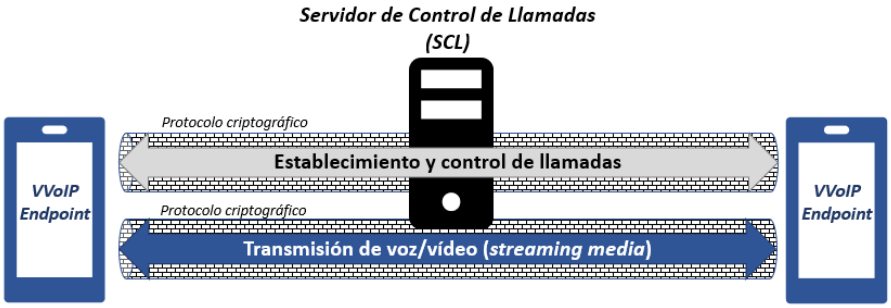

Figura 1 – Arquitectura cliente-servidor.

2.2.2. CASO DE USO 2 – ARQUITECTURA P2P

15. La arquitectura del producto es extremo a extremo (P2P, peer-to-peer). Cada VVoIP endpoint interactúa directamente con otros VVoIP endpoints sin necesidad de utilizar ningún Servidor de control de llamadas de intermediario, ya que esta función la proporciona el propio VVoIP endpoint.

16. En este caso de uso, es el VVoIP endpoint el encargado de las funciones de auditoría del sistema, incluido el registro de los detalles de las llamadas o CDRs (*Call Details Records*).

Figura 2 – Arquitectura P2P.

2.3 ENTORNO DE USO

17. Para la utilización en condiciones óptimas de seguridad de la Herramienta de comunicaciones VoIP/VVoIP, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

    - **Protección física**. El producto debe estar protegido físicamente por su entorno operacional y no sujeto a ataques físicos que puedan comprometer su seguridad o interferir en su correcta operación. En caso de productos software, esta hipótesis aplica a la plataforma física sobre la que se ejecuta el producto.
    - **Administración confiable:** Los administradores son miembros de plena confianza y velan por los mejores intereses en materia de seguridad de la organización. Dichas personas deben estar debidamente capacitadas y carecer de cualquier intención maliciosa o conflicto de intereses al administrar el producto.
    - **Actualizaciones periódicas.** El *firmware/software* del producto es actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
    - **Funcionalidad limitada.** El producto solo debe proporcionar la funcionalidad de control de llamadas y transmisión de voz/vídeo, 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

18. Este tipo de productos se presentan:
    a) El VVoIP endpoint puede presentarse como un dispositivo hardware dedicado con capacidad VVoIP, o como una aplicación VVoIP que se ejecuta en un dispositivo hardware de propósito general.
    b) El Servidor de control de llamadas (SCL) puede presentarse como un *appliance* dedicado con un firmware no modificable, o como un servidor de propósito general que proporciona la funcionalidad de control de llamadas.

2.5 CERTIFICACIÓN LINCE

19. Para que un producto de esta familia pueda ser incluido en el CPSTIC bajo la categorización de ENS Categoría MEDIA, deberá disponer de una Certificación Nacional Esencial de Seguridad (LINCE)[1] que incluya los RFS reflejados en el apartado 4, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.
20. El alcance de la evaluación deberá incluir el módulo de evaluación básico de 25 días de esfuerzo y el Módulo de Evaluación Criptográfica (MEC). El Módulo de Revisión de Código Fuente (MCF) será opcional.

[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

21. La convención utilizada en las descripciones es la siguiente:

    - Selección**:** se deberá seleccionar al menos una opción de las indicadas y se incluirá en la declaración de seguridad. Ejemplo:

      AC.PSC. [**selección**: credenciales; claves] que deben ser protegidos en Confidencialidad e Integridad.

      DS: **AC.PSC**. credenciales que deben ser protegidos en Confidencialidad e Integridad.

    - Asignación: se deberá especificar el listado de opciones que sean de aplicación al TOE (podría no haber ninguna). Ejemplo:

      AC.PSS. Datos de configuración, registros de auditoría y [**asignación**: listado de datos definidos por el fabricante] que deben ser protegidos en Integridad.

      DS: **AC.PSS**. Datos de configuración, registros de auditoría que deben ser protegidos en Integridad.

22. 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 de 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

23. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente, atendiendo a los casos de uso expuestos 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.
- **A.VVoIP Endpoints no autorizados**: Un atacante puede intentar registrar un VVoIP endpoint no autorizado, con el propósito de suplantar a un usuario legítimo y establecer conexiones no autorizadas con otros VVoIP endpoints o con llamadas activas.

3.3 TRAZABILIDAD AMENAZAS / REQUISITOS DE SEGURIDAD

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

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.PSC	A.FUN	A.NOAUTUSR	A.CRE	A.VVOIP
VVoIP.1			X							
VVoIP.2										X
VVoIP.3		X	X							
VVoIP.4		X	X							
VVoIP.5		X	X							
VVoIP.6										X
VVoIP.7										X
VVoIP.8					X					
SCL.1										X
SCL.2		X	X							
SCL.3					X					
SCL.4					X					
SCL.5					X					
SCL.6										X
SCL.7				X						
SCL.8					X					

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

24. 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.

25. 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.

26. El apartado 4.1 indica los requisitos que debe cumplir el **VVoIP endpoint**. El apartado 0 indica los requisitos que debe cumplir el **servidor de control de llamadas** para los casos de arquitecturas cliente-servidor (caso de uso 1).

4.1 VVOIP ENDPOINT

4.1.1. ADMINISTRACIÓN CONFIABLE

27. Podrán ser cubiertas por el producto o por su entorno operacional.

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

29. **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].

30. **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.

4.1.2. IDENTIFICACIÓN Y AUTENTICACIÓN

31. Podrán ser cubiertas por el producto o por su entorno operacional.
32. **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*].
33. **IAU.2** El TOE deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
34. **IAU.3** El TOE debe disponer de la capacidad de gestión de las contraseñas:
    a) La contraseña debe de poder configurarse con una longitud mínima o igual a 12 caracteres.
    b) La contraseña debe ser capaz de componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “]

> Nota de aplicación: este requisito podría ser modificado en el caso de que el TOE implemente otros mecanismos de autenticación.

35. **IAU.4** El TOE debe [**selección***: bloquear; cerrar*] la sesión de un usuario después de [***asignación****: tiempo de inactividad*] de inactividad.
36. **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.

4.1.3. CANALES SEGUROS

37. Podrán ser cubiertas por el producto o por su entorno operacional.
38. **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*].
39. **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.
40. **COM.3** El TOE hará uso de certificados digitales para la autenticación cuando utilice cualquiera de los protocolos definidos en **COM.1**.
41. **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*].

4.1.4. INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

42. **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].
43. **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.
44. **ACT.3** En caso de que el TOE sea un dispositivo hardware, la actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.

4.1.5. AUDITORÍA

45. Podrán ser cubiertas por el producto o por su entorno operacional. Serán obligatorias cuando el TOE actúe de servidor de control de llamadas (arquitectura P2P, caso de uso 2).
46. **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].
47. **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.
48. **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]
49. **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].

50. **AUD.5** El TOE deberá [**selección**: sobrescribir 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.

4.1.6. PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

51. **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**.

4.1.7. CRIPTOGRAFÍA

52. Podrán ser cubiertas por el producto o por su entorno operacional.
53. **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.
54. **CIF.2.** Generador de bits aleatorios. En caso de suministrar un servicio de generación de bits aleatorios (RBG[2]) determinísticos, el producto deberá:
    - Utilizar [**selección:** *Hash_DRBG (any), HMAC_DRBG (any)* o *CTR_DRBG (AES)*].
    - Usar una semilla de, al menos, una Fuente de entropía que acumule entropía [selección: de una o varias fuentes; una Fuente de entropía estudiada], con un mínimo de bits de entropía al menos igual a la mayor Fortaleza de seguridad de las claves y hashes que generará, de acuerdo a la ISO/IEC 18031:2011.

[2] *Random Bit Generator*

4.1.8. VVOIP

55. **VVoIP.1** En caso de que el TOE se comunique con un servidor de control de llamadas (arquitectura cliente-servidor, caso de uso 1), deberá utilizar el protocolo de nivel de aplicación [**selección**: *Session Initiation Protocol (SIP); H.323*] para establecer un canal seguro entre sí mismo y el servidor de control de llamadas.

56. **VVoIP.2** En caso de que el TOE actúe como servidor de control de llamadas (arquitectura P2P, caso de uso 2), solo permitirá el establecimiento de llamadas entre sí mismo y otro VVoIP endpoint, cuando el identificador [**asignación**: *método por el que el TOE identifica cada endpoint para una llamada*] sea válido, según el protocolo de control de llamada [**selección**: *SIP; H.323*].

57. **VVoIP.3** El TOE deberá utilizar el protocolo de nivel de aplicación [**selección**: *Secure Real-Time Transport Protocol (SRTP); H235/H.323*] para establecer un canal seguro entre sí mismo y otro VVoIP endpoint u otro dispositivo de telefonía, para la transmisión de voz/vídeo.

58. **VVoIP.4** El TOE deberá utilizar el protocolo de nivel de transporte TLS 1.2 o superior, para proteger la información de control de llamadas y la transmisión de voz/vídeo. La autenticación será mutua y hará uso de certificados digitales X.509v3. Los mecanismos criptográficos utilizados por TLS, deberán ser acordes con el requisito CIF.1.

59. **VVoIP.5** En caso de que el TOE utilice SRTP como protocolo para la transmisión de voz/video, la implementación del protocolo debe seguir el estándar de la RFC 3711, debe utilizar SDES (*Security Descriptions for Media Streams*) para la negociación de claves criptográficas de la conexión SRTP según indica la RFC 4568, y debe utilizar mecanismos criptográficos acordes con el requisito CIF.1.

60. **VVoIP.6** El TOE solo debe transmitir voz/vídeo cuando se cumplan todas las siguientes circunstancias:

    a) [**selección**: *el TOE se ha registrado como VVoIP endpoint en un servidor de control de llamadas (arquitectura cliente-servidor, caso de uso 1); el TOE actúa como servidor de control de llamadas (arquitectura P2P, caso de uso 2)*].
    b) Se ha establecido una llamada con otro VVoIP endpoint.
    c) El TOE está en estado off-hook (descolgado).
    d) El TOE no está en estado mute.

61. **VVoIP.7** El TOE debe finalizar una transmisión de voz/vídeo después de un periodo de inactividad [**selección**: [**asignación**: *tiempo (en segundos) por defecto*] *segundos; tiempo configurable por el administrador*].

    NOTA: Si se selecciona “tiempo configurable por el administrador”, este tiempo debe poder configurarse en ADM.2.

62. **VVoIP.8** En caso de que el TOE actúe como servidor de control de llamadas (arquitectura P2P, caso de uso 2), debe generar registros de auditoría cuando se produzca alguno de los siguientes eventos:

- Con cada llamada que se establezca, guardando un registro (CDR, *Call Detail Records*) que contenga: identificación del llamante, identificación del llamado, fecha/hora de inicio y fin de la llamada y duración de la misma.
- Con la finalización de una llamada por tiempo de inactividad, guardando un registro que contenga: identificación del llamante, identificación del llamado, fecha/hora de inicio de la llamada, fecha/hora en la que se termina la llamada por tiempo de inactividad, y duración total de la misma.

4.2 SERVIDOR DE CONTROL DE LLAMADAS (SCL)

4.2.1. ADMINISTRACIÓN CONFIABLE

63. Podrán ser cubiertas por el TOE o por su entorno operacional.
64. **ADM.1** El TOE debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.
65. **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].
66. **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.

4.2.2. IDENTIFICACIÓN Y AUTENTICACIÓN

67. Podrán ser cubiertas por el producto o por su entorno operacional.
68. **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*].
69. **IAU.2** El TOE deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.
70. **IAU.3** El TOE 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 [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “]

> Nota de aplicación: este requisito podría ser modificado en el caso de que el TOE implemente otros mecanismos de autenticación.

71. **IAU.4** El TOE debe [**selección***: bloquear; cerrar*] la sesión de un usuario después de [asignación: tiempo de inactividad] de inactividad.
72. **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.

4.2.3. CANALES SEGUROS

73. Podrán ser cubiertas por el producto o por su entorno operacional.
74. **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*].
75. **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.
76. **COM.3** El TOE hará uso de certificados digitales para la autenticación cuando utilice cualquiera de los protocolos definidos en COM.1.
77. **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*].

4.2.4. INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

78. **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].
79. **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.
80. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.

4.2.5. AUDITORÍA

81. Podrán ser cubiertas por el producto o por su entorno operacional.
82. **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.
    c) Cambio 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].
83. **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.
84. **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: [**selección**: solo administradores; ningún usuario]
85. **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].
86. **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.

4.2.6. PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

87. **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.

4.2.7. PROTECCIÓN DEL PRODUCTO Y SUS SERVICIOS

88. **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*].

4.2.8. CRIPTOGRAFÍA

89. Podrán ser cubiertas por el producto o por su entorno operacional.

90. **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.

91. **CIF.2** Generador de bits aleatorios. En caso de suministrar un servicio de generación de bits aleatorios (RBG) determinísticos, el TOE deberá:

    - Utilizar [**selección**: Hash_DRBG (any), HMAC_DRBG (any) o CTR_DRBG (AES)].

92. Usar una semilla de, al menos, una fuente de entropía que acumule entropía [selección: de una o varias fuentes; una fuente de entropía estudiada], con un mínimo de bits de entropía al menos igual a la mayor fortaleza de seguridad de las claves y hashes que generará, de acuerdo a la ISO/IEC 18031:2011.

4.2.9. CONTROL DE LLAMADAS

93. **SCL.1** El TOE solo permitirá el establecimiento de llamadas entre VVoIP endpoints, cuando el identificador [**asignación**: *método por el que el TOE identifica cada endpoint para una llamada*] sea válido, según el protocolo de control de llamada [**selección**: *SIP; H.323*]. Una vez determina la llamada como válida, el TOE establecerá (a) una conexión entre sí mismo y el llamante, (b) una segunda conexión entre sí mismo y el llamado y (c) redirigirá todas las comunicaciones entre los dos VVoIP endpoints, a través de la conexión adecuada.

94. **SCL.2** El TOE deberá utilizar el protocolo de nivel de transporte TLS 1.2 o superior, para proteger el canal de comunicación con los VVoIP endpoint (para señalización y para envío de voz/vídeo). La autenticación será mutua y hará uso de certificados digitales X.509v3. Los mecanismos criptográficos utilizados por TLS, deberán ser acordes con el requisito CIF.1.

95. **SCL.3** El TOE debe proporcionar referencias de tiempo fiables mediante la sincronización de la fecha/hora con un servidor NTP, utilizando el protocolo NTP v4 (RFC 5905).

96. **SCL.4** El TOE debe generar un registro de detalles de llamadas (CDR, *Call Detail Record*) para las comunicaciones que establezca entre los VVoIP endpoint. Cada registro debe contener, al menos, la siguiente información: identificación del llamante, identificación del llamado, fecha/hora de inicio y fin de la llamada, y duración de la misma.

97. **SCL.5** El TOE protegerá y almacenará los registros de llamadas (CDRs), según se indica en los requisitos AUD.3, AUD.4 y AUD.5.

98. **SCL.6** El TOE debe tener la capacidad de mostrar el estado de las conexiones de todos los VVoIP endpoints en tiempo real.

99. **SCL.7** En caso de que sea el TOE el responsable de entregar las actualizaciones de software/firmware a los VVoIP endpoints (esta funcionalidad puede ser delegada en otro servidor de la organización), deberá cumplir los requisitos ACT.1, ACT.2 y ACT.3 en relación con las actualizaciones de los VVoIP endpoints.

100. **SCL.8** En caso de que el TOE tenga la capacidad de grabar las llamadas de voz/vídeo:

- Debe identificar cada grabación de forma unívoca utilizando el siguiente método [**asignación**: *dato de identificación única*].
- Debe almacenar los registros de grabación en formato [**asignación**: *formato de fichero soportado*].
- Debe llevar a cabo la retención de las grabaciones de voz/vídeo según el siguiente criterio [**asignación**: *criterio especificado por el administrador*].
- Debe impedir toda modificación de las grabaciones de voz/vídeo almacenadas, y protegerlas de lecturas no autorizadas mediante mecanismos de cifrado acordes con CIF.1.
- Debe permitir habilitar y deshabilitar la grabación de voz/vídeo para cualquier VVoIP endpoint registrado.

4.3 NOTAS DE APLICACIÓN

101. En el Caso de Uso 1 – Arquitectura cliente-servidor SCL, los requisitos deberán aplicarse tanto al Cliente como al servidor de control de llamadas (SCL). Por tanto, el alcance de la certificación deberá incluir ambos: el Cliente y el servidor de control de llamadas (SCL).

5. ABREVIATURAS

CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de Información y las Comunicaciones
EAL	*Evaluation Assurance Level*
ENS	Esquema Nacional de Seguridad
NIAP	*National Information Assurance Partnership*
RFS	Requisitos Fundamentales de Seguridad
SCL	Servidor de Control de Llamadas
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