CCN
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo D.9BM: Herramientas de Mensajería Instantánea (IM)

Julio 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 CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.07.13 12:55:42 +02'00'

NIPO: 083-23-071-5
Fecha de Edición: julio 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 Mensajería Instantánea (IM, *Instant Messaging*)** 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 Mensajería Instantánea (IM)** 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 **Herramientas de Mensajería Instantánea (IM, *Instant Messaging*)** a todo producto que permita a dos o más participantes establecer una comunicación para mensajería y transferencia de archivos, a través de cualquier tipo de red (celular, Wi-Fi, etc.). Esta comunicación debe ser segura, es decir, implementará mecanismos para garantizar la autenticación de emisor y receptor y la confidencialidad e integridad de la información transmitida.
7. El funcionamiento de estas herramientas normalmente consiste en que el usuario emisor introduce el texto, y solicita su envío a uno o varios receptores conectados a una red común. Este tipo de comunicación basada en texto suele llamarse chat, y puede establecerse entre dos participantes (chat privado) o más participantes (chat grupal). Generalmente tienen lugar en tiempo real, aunque existen modalidades de mensajería offline.
8. Además del intercambio de mensajes de texto, estas herramientas suelen presentar funcionalidades adicionales, como:
    - Confirmación (ack) al emisor, del envío, entrega y/o lectura del mensaje por parte del receptor.
    - Intercambio de ficheros adjuntos (*attachments*) de diversos tipos y formatos (incluidos audios o vídeos).
    - Eliminación del mensaje enviado a petición del emisor (revocación), o tras un periodo de tiempo definido por el emisor. Generalmente esto solo es posible cuando el mensaje aún no ha sido leído por el receptor.
    - Indicador de presencia, que muestra la disponibilidad en tiempo real de los participantes de chats privados o grupales.
    - Almacenamiento de las conversaciones y de los ficheros adjuntos.
9. Generalmente estas herramientas ofrecen también llamadas de voz y vídeo entre dos participantes o conferencias entre varios participantes (*conference calls*). **Esta funcionalidad VVoIP no entra dentro del presente Anexo**, sino que se encuentra recogida en el Anexo de Herramientas de comunicaciones VVoIP.
10. Aunque no son estrictamente herramientas de mensajería instantánea, **se considerarán dentro del presente Anexo, las herramientas de mensajería offline**. Estas son aquellas que permiten al emisor enviar un mensaje que se queda almacenado offline, a la espera de que el receptor reciba la notificación de que tiene un mensaje y acceda a dicho mensaje.

2.2 CASOS DE USO

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

2.2.1. CASO DE USO 1 – ARQUITECTURA CLIENTE-SERVIDOR CON APLICACIÓN CLIENTE

12. La arquitectura del producto está formada por un cliente que se conecta a un **Servidor de Mensajería Instantánea** (**IMS**, *Instant Message Server*).
13. El **cliente es una aplicación software** que se instala en el dispositivo móvil o en un PC. Cuando un usuario envía un mensaje a otro usuario, la aplicación cliente envía el mensaje al Servidor IMS, que almacena el mensaje y lo entrega al usuario destino cuando este se encuentre disponible. El servidor IMS generalmente tiene un límite de tiempo configurable durante el cual almacena los mensajes y ficheros y, después, los borra.
14. En este tipo de arquitectura, generalmente es el Servidor IMS el que proporciona las funciones de: configuración y gestión de la herramienta, autenticación de usuarios, distribución de actualizaciones, auditoría y almacenamiento seguro de mensajes y ficheros. El resto de funciones de seguridad: protección de las comunicaciones, protección de credenciales y criptografía son proporcionadas, también, por la aplicación cliente.

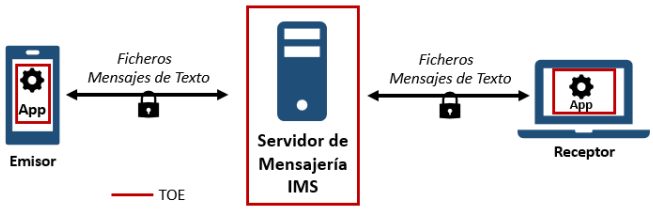

Figura 1 – Arquitectura Cliente-Servidor con App cliente

2.2.2. CASO DE USO 2 – ARQUITECTURA P2P SIN SERVIDOR (*SERVLESS*)

15. La arquitectura del producto es extremo a extremo (P2P, *peer-to-peer*), también llamada "*servless*" (sin Servidor IMS). El producto es una **aplicación software** que se instala en un dispositivo móvil o PC, e interactúa directamente con otras aplicaciones de mensajería sin necesidad de utilizar ningún Servidor IMS de intermediario.
16. En este caso, es la aplicación de mensajería la encargada de implementar todas las funciones de seguridad.

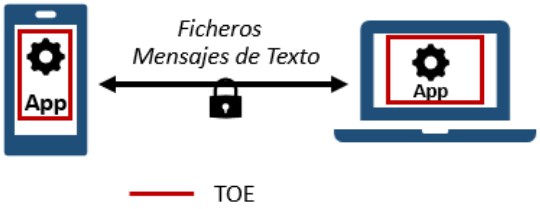

Figura 2 – Arquitectura P2P

2.3 ENTORNO DE USO

17. Para la utilización en condiciones óptimas de seguridad de la Herramienta de Mensajería Instantánea, 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 mensajería instantánea, como función principal, opcionalmente llamadas de voz/vídeo, 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:
    - La parte cliente suele presentarse como una aplicación software o simplemente un navegador web (web browser).
    - El Servidor IMS puede presentarse:
        i. En formato on-premise: como un *appliance* dedicado con un firmware no modificable o como una aplicación software que se ejecuta en un servidor de propósito general.
        ii. En formato de servicio en la nube.

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 2.2, serían:

- **A.NOAUT Acceso no autorizado de administrador**: Un atacante puede obtener un acceso de administración no autorizado haciéndose pasar por un administrador ante el producto, haciéndose pasar por el producto ante un administrador, reproduciendo una sesión de administración, o realizando ataques del hombre en medio.
- **A.CRYPTO Mecanismos criptográficos débiles**: Utilización en el producto de mecanismos criptográficos o longitudes de clave débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
- **A.COM Protocolos de comunicación no autorizados**: Utilización de protocolos no autorizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones críticas del producto.
- **A.ACT Actualización maliciosa**: un atacante puede realizar una actualización maliciosa que comprometa las funcionalidades del producto.
- **A.AUD Actividades no detectadas**: Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador.
- **A.INT Compromiso de la integridad del software/firmware:** Un atacante puede intentar comprometer la integridad del producto a través de un software sin privilegios ejecutado en la misma plataforma en la que se ejecuta el producto.
- **A.PSC Compromiso de parámetros de seguridad críticos:** Un atacante puede comprometer los parámetros de seguridad críticos y acceder de forma continuada al producto y a sus datos críticos.
- **A.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.CON Compromiso de credenciales**: Un atacante puede aprovecharse del uso credenciales débiles o desprotegidas, para ganar acceso privilegiado al producto.
- **A.IM Acceso no autorizado a mensajes y ficheros:** Un atacante puede obtener un acceso no autorizado a mensajes o ficheros de usuarios legítimos, almacenados en el producto.

3.3 TRAZABILIDAD AMENAZAS / REQUISITOS DE SEGURIDAD

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.INT	A.PSC	A.FUN	A.NOAUTUSR	A.CON	A.IM
ADM.1	X										
ADM2	X										
ADM.3	X										
IAU.1	X								X		
IAU.2										X	
IAU.3										X	
IAU.4	X										
IAU.5										X	
COM.1		X	X								
COM.2			X								
COM.3			X								
COM.4		X	X								
ACT.1				X							
ACT.2				X							
ACT.3				X							
ACT.4				X							
ACT.5				X							
AUD.1					X						
AUD.2					X						
AUD.3					X						
AUD.4					X						
AUD.5					X						
EXP.1						X					
EXP.2						X					
EXP.3						X					
PSC.1							X				
PRO.1								X			
CIF.1		X	X								
CIF.2		X	X								
IM.1		X	X								
IM.2	X								X		X
IM.3											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. Como se indica en algunos casos, las funciones de seguridad solicitadas en los RFS pueden ser proporcionadas por el entorno operacional. En caso de que sea el producto el que proporciona estas funciones de seguridad, estas podrán ser implementadas por la Aplicación cliente, por el Servidor IMS o por ambos, dependiendo de la arquitectura del producto tal y como se indica en los Casos de Uso.

4.1 ADMINISTRACIÓN CONFIABLE

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

28. **ADM.1** El TOE debe 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.

4.2 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 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.

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.

4.3 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*].

4.4 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** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.
45. **ACT.4** En el caso de que el TOE sea una aplicación *software*, esta deberá estar empaquetada de forma que, si se elimina, no deje rastro de su instalación (excepto por configuraciones y ficheros de salida o auditoría).
46. **ACT.5** En el caso de que el TOE sea una aplicación *software*, este no descargará ni modificará su propio código binario.

4.5 AUDITORÍA

47. Podrán ser cubiertas por el producto o por su entorno operacional.
48. **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*].
49. **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.

50. **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*]
51. **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*].
52. **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.

4.6 CAPACIDADES ANTI-EXPLOTACIÓN

53. **EXP.1** En el caso de que el TOE sea una aplicación *software*, cuando el TOE se encuentre en ejecución, este no solicitará la asignación de ninguna dirección explícita de memoria del sistema, ni asignará memoria con permisos simultáneos de escritura y ejecución.
54. **EXP.2** En el caso de que el TOE sea una aplicación *software*, estará configurado por defecto con permisos de ficheros que lo protejan de accesos no autorizados.
55. **EXP.3** En el caso de que el TOE sea una aplicación *software*, este solamente utilizará las bibliotecas de terceras partes declaradas [**asignación**: *listado de librerías*].

4.7 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

56. **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

57. **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 CRIPTOGRAFÍA

58. Podrán ser cubiertas por el producto o por su entorno operacional.
59. **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.
60. **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)].
    - 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.

4.10 MENSAJERÍA INSTANTÁNEA

61. **IM.1** El envío de mensajes de texto y ficheros, se llevará a cabo por un canal seguro tal y como establece el requisito COM.1, y utilizando mecanismos criptográficos que cumplan con el requisito CIF.1.
62. **IM.2** El TOE deberá autenticar a cada usuario antes de permitirle el establecimiento de una comunicación con otros usuarios.
63. **IM.3** En caso de que el TOE almacene mensajes y/o ficheros, estos solo serán accesibles por los usuarios autorizados (emisor y receptor), y no serán accesibles por ningún otro usuario ni administrador.

4.11 NOTAS DE APLICACIÓN

64. En el Caso de Uso 1, arquitectura cliente-servidor con aplicación cliente, los requisitos deberán aplicarse tanto al Cliente como al **Servidor de Mensajería Instantánea** (**IMS**, *Instant Message Server*). Por tanto, el alcance de la certificación deberá incluir ambos: el Cliente y el servidor de Mensajería IMS.

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
SCL	Servidor de Control de Llamadas
NIAP	*National Information Assurance Partnership*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*
TOE	*Target of Evaluation*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL