centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 1407

## Procedimiento de empleo seguro de COMSec

Octubre de 2019

MINISTERIO DE DEFENSA

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.11.21 16:55:01 +01'00'


NIPO: 083-19-058-6

Fecha de Edición: Octubre de 2019
INDRA SCS ha participado en la realización y modificación del presente documento y sus anexos.

# PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Julio de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

# ÍNDICE

# LISTADO DE FIGURAS

# 1 INTRODUCCIÓN

1. El sistema COMSec integra un sistema de comunicaciones móviles seguras. COMSec ofrece servicios de comunicaciones con cifrado extremo a extremo de voz y vídeo, mensajería, así comotransferencia de archivos entre usuarios del sistema.

## 1.1 PROPÓSITO

2. El presente documento describe los pasos a seguir para desplegar y poner en marcha el sistema COMSec v3.21 de acuerdo con las directrices establecidas por el Centro Criptológico Nacional durante el proceso de cualificación del producto. El seguimiento de las directrices y configuraciones incluidas en el presente documento es obligatorio para mantener el nivel de seguridad
3. También incluye los aspectos de seguridad del sistema y ofrece una guía de uso de las aplicaciones cliente.

## 1.2 AMBITO DE APLICACIÓN

4. El presente documento debe ser conocido tanto por el Administrador del Sistema como por el Administrador de Claves del Sistema COMSec dentro de la organización que despliega el sistema.

# 2 DESCRIPCIÓN DEL SISTEMA

5. El sistema COMSec proporciona comunicaciones cifradas de voz, video y mensajería instantánea a usuarios móviles a través de una aplicación instalada en una plataforma Android.

6. El sistema hace uso de un servidor de comunicaciones que ofrece servicio a los usuarios móviles, de manera que puedan funcionar de manera autónoma.

## 2.1 COMPONENTES DEL SISTEMA

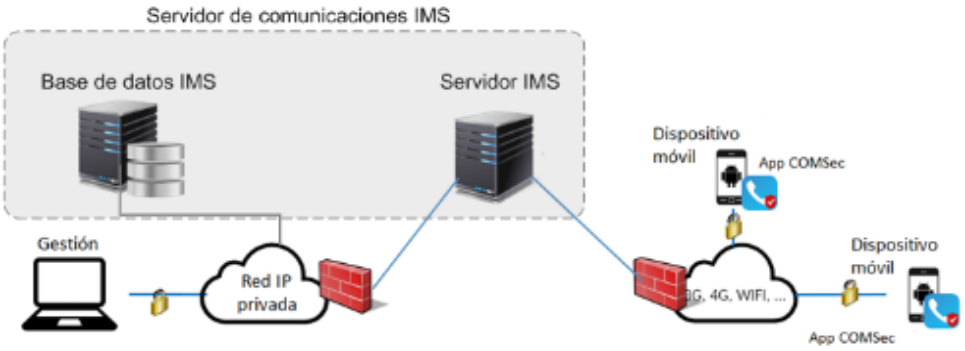


*Figura 1. Arquitectura del sistema*

## 2.2 SERVIDOR DE COMUNICACIONES COMSEC (IMS)

7. Es un servidor centralizado de comunicaciones que proporciona la infraestructura para proveer de comunicaciones seguras a los usuarios finales del sistema.

8. Se compone principalmente de:

   - **Servidor IMS**: modulo principal que gestiona la conectividad y la lógica de la aplicación COMSec.
   - **Base de datos**: componente para el almacenamiento de datos del servidor IMS.

### 2.2.1 APLICACIÓN COMSEC

9. Es una aplicación de usuario para dispositivos con sistema operativo Android. Proporciona comunicaciones seguras entre usuarios. Las diferentes funcionalidades ofrecidas son: llamadas de voz y vídeo, mensajería y transferencia segura de archivos.

### 2.2.2 COMPONENTES AUXILIARES

10. Dispositivo móvil: El dispositivo donde se ejecute COMSec debe ser un terminal con sistema operativo Android (versión 5.1.1 o superior), listado cómo producto cualificado en el Catálogo de Productos de Seguridad TIC (CPSTIC) [3] en la familia de dispositivos móviles y pertenecer a un despliegue corporativo con las condiciones de seguridad adecuadas, debiendo cumplir con directrices marcadas en la guía CCN-STIC 496 Sistemas de Comunicaciones Móviles Seguras [4].

11. Centro de gestión: Ordenador en la red interna de la organización con conectividad con el servidor IMS donde se realizan las tareas de gestión y administración del sistema COMSEC. El equipo debe tener instalado un navegador web con todos los parches de seguridad aplicados.

# 3 ARQUITECTURA DE SEGURIDAD

12. Para que la aplicación COMSec pueda conectarse al servidor IMS, es necesario completar un proceso de autenticación entre ambas partes. A partir de este proceso, se establecerá un canal de señalización que permitirá asegurar el intercambio de datos cifrados, así como su integridad.

13. Se distinguen dos tipos de tráfico de datos entre el servidor IMS y los dispositivos móviles:

    - Canal de control y señalización
    - Canal de datos de usuario


*Figura 2. Pila de protocolos establecidos en el canal COMSec*

## 3.1 CANAL DE SEÑALIZACIÓN

14. El canal de señalización es el utilizado para la comunicación entre la aplicación COMSec y el servidor IMS. Por él se transmiten tanto los comandos de señalización necesarios para, el establecimiento y control de llamadas, envío de listas de contactos, control de registro y presencia, etc. Este canal se asienta sobre el protocolo de transporte TCP (debido, principalmente, a su fiabilidad en la transmisión de datos) y, sobre él, se establecen una serie de capas de cifrado que introducen las capacidades de autenticación, confidencialidad e integridad de los datos enviados. De esta manera se consigue que, a nivel de red, las comunicaciones sobre este canal sean inviolables y seguras.

### 3.1.1 AUTENTICACIÓN TLS

15. Para utilizar este tipo de autenticación es necesario disponer de una infraestructura de clave pública (PKI) que permita la identificación de las partes basándose en certificados digitales x5091.

16. El protocolo implementado es el estándar TLS v1.2 (Transport Layer Security) que ofrece no sólo la autenticación de las partes, sino que además proporciona cifrado e integridad de los datos intercambiados.

17. El canal TLS se establece únicamente tras la correcta validación del certificado digital presentado por la parte servidora (IMS). Esto tiene como resultado la simplificación del proceso de provisión de usuarios/dispositivos, siendo suficiente el despliegue de los certificados de CA raíz necesarios para validar al Operador Virtual IMS.

[1] Formato estándar para certificados de clave pública / privada

# 4 CLAVES Y CERTIFICADOS

## 4.1 TIPOS DE CLAVES. GENERACIÓN, DISTRIBUCIÓN Y CARGA.

18. El sistema COMSec requiere del uso de certificados digitales X.509 v.3 para la autenticación entre los usuarios móviles y el servidor IMS, así como para la autenticación entre servidores IMS para establecer comunicaciones seguras con otras organizaciones.

19. El servidor IMS cuenta con una PKI (Infraestructura de clave pública) capaz de generar y gestionar todos los certificados empleados por el sistema de forma autónoma empleando las herramientas proporcionadas por el desarrollador del sistema. El IMS es capaz de aceptar el uso de una PKI externa.

20. Para asegurar la correcta gestión de claves, todos los componentes del sistema COMSEC deben ser mantenidos con la fecha y hora correctas.

21. Como norma general, las claves deben ser manejadas de acuerdo con la normativa aplicable a su nivel de clasificación.

22. El sistema COMSec utiliza los siguientes tipos de claves:

**Contraseña de un solo uso OTP (*One Time Password*):** es una contraseña temporal que se genera a través de la consola de gestión del IMS y sirve para enrolar nuevos clientes COMSec al IMS. El administrador del sistema se encarga de distribuir esta contraseña al usuario final. Con esta contraseña y con el nombre de usuario se establece una conexión limitada con el IMS. Durante esta conexión sólo se permite el establecimiento de una nueva contraseña que sólo conocerá el usuario final del sistema COMSec. Estas contraseñas se usan para las altas nuevas de usuarios al sistema o cuando un usuario notifica al administrador que ha olvidado su contraseña COMSec.

**Credenciales de acceso (usuario y contraseña) a la aplicación COMSec** empleados por el usuario final para autenticarse y acceder a la aplicación móvil. El usuario es definido por el administrador del sistema en el momento de la creación del mismo y no puede ser modificado**.** La contraseña de usuario debe de ser sólo conocida por el usuario y debe además ser difícil de predecir. Recordar la contraseña es responsabilidad del usuario. Si el usuario olvida su contraseña deberá ponerse en contacto con el Administrador para que le proporcione una nueva OTP. La longitud de la contraseña de usuario deberá ser como mínimo de 12 caracteres alfanuméricos y debe contener letras mayúsculas y minúsculas, números y símbolos. La política de contraseñas no permite secuencias predecibles, tales como *1234…* o *abcd….*

**Contraseña de copia de seguridad de datos de la aplicación.** Contraseña empleada para cifrar la copia de respaldo de datos de la aplicación. Esta contraseña la elige el usuario final y debe deberá ser compleja y de al menos 6 caracteres alfanuméricos, incluyendo letras mayúsculas, minúsculas y números. Si el usuario olvida esta contraseña, no podrá restaurar posteriormente las copias de seguridad de la Base de Datos del terminal.

**Credenciales de acceso (usuario y contraseña) para la gestión web del IMS.** Deberá atenderse la directiva de contraseñas reflejadas en el Ref. [2] *CCNSTIC 521*

*Configuración segura de Windows Server 2008 R2*. Configuración segura de Windows Server 2008 R2: contraseña compleja de longitud mínima 12 caracteres.

**Certificado de servidor IMS.** Es el certificado empleado por el IMS para autenticarse con los usuarios móviles (aplicación COMSec) y, en caso de que el sistema esté conectado a otros sistemas COMSec externos, con otros servidores IMS. Dependiendo de si el sistema funciona de forma aislada o está conectado con otros sistemas COMSec, este certificado puede ser de dos tipos:

- **Certificado de servidor IMS aislado**. Es el certificado usado por el IMS para autenticarse con los usuarios de la aplicación móvil COMSec. Es un fichero con certificado del servidor IMS y clave privada asociada en formato **PKCS12** (extensión *pfx*). El certificado propio debe contener el campo SAN (*Subject Alternative Names*), la IP externa o el DNS del IMS al que se conecta la aplicación COMSec. La aplicación comprueba en cada conexión que este campo existe en el certificado que presenta el IMS y además coincide con la IP o DNS a la que la aplicación se conecta.
- **Certificado de servidor IMS federable**. Es el certificado usado por el IMS para autenticarse con los usuarios de la aplicación móvil COMSec y con otros servidores IMS, en el caso de un sistema federable. El certificado es similar al Certificado de servidor IMS aislado con la particularidad de que no tiene la restricción de servidor y es capaz de iniciar conexiones hacia otros servidores.

**Certificado de CA**. Un fichero (o varios) con los certificados de CA necesarios para validar la cadena de certificación del certificado de IMS.

23. Los certificados de CA que validan del certificado de IMS están embebidos en la aplicación COMSec. Éstos sólo se usarán para validar la cadena de certificación del certificado de IMS en el establecimiento del canal TLS entre IMS y cliente COMSec.

24. Se podrán comprobar las CAs de aplicación en el menú Seguridad -> Certificados de aplicación.

25. Si el IMS se conecta a sistemas COMSec de otras organizaciones, serán necesarios también los certificados de CA de la cadena de certificación de los IMS federados.

## 4.2 CICLO DE VIDA Y ACTUALIZACIÓN DE CLAVES.

26. El ciclo de vida del material criptográfico es el marco temporal durante el cual este material tiene validez. Los ciclos de vida deben ser acortados en proporción al daño potencial que podría resultar del compromiso del activo protegido por una clave.

27. A continuación, se describen los ciclos de vida recomendados para el diferente material criptográfico:

- **Contraseña de un solo uso OTP.** Tendrá una validez de 7 días. Tras este periodo, si no se ha utilizado el OTP no será válido y deberá solicitarse uno nuevo.
- **Credenciales de acceso (usuario y contraseña) a la aplicación COMSec**. La contraseña de acceso a la aplicación móvil deberá modificarse al menos cada 90 días.
- **Contraseña de copia de seguridad de Base de datos** de usuario de la aplicación. Esta contraseña será de un solo uso.

- **Credenciales de acceso (usuario y contraseña) para la consola de administración web del IMS**. La contraseña de acceso a la consola de administración web del servidor IMS deberá modificarse al menos cada 90 días.
- **Certificado de servidor IMS (aislado o federable).** El certificado de servidor tendrá una duración máxima de 5 años.
- **Certificado de CA (raíz o intermedia).** El certificado de CA del sistema COMSec tendrá una duración máxima de 10 años.

# 5 PROCEDIMIENTO DE EMERGENCIA

28. La salvaguarda de los dispositivos del Sistema COMSEC (terminales de usuario final, servidor IMS, PC de gestión) y el material COMSEC asociado bajo condiciones de emergencia son responsabilidad del poseedor de los mismos y del responsable del sistema.

## 5.1 DESTRUCCIÓN DE UN TERMINAL DE USUARIO DE COMSEC

29. Cuando el usuario de una aplicación COMSec tenga una sospecha razonable de que su dispositivo móvil ha podido ser comprometido o manipulado, debe:
    - Avisar al Administrador del sistema para recibir instrucciones
    - No volver utilizar el sistema hasta que su Administrador le autorice a ello tras realizar las comprobaciones oportunas.
30. El Administrador del sistema puede decidir incluir como protocolo la realización de un borrado de emergencia tan pronto como sea posible, para realizarlo, sería necesario acudir al apartado Ajustes, Cerrar sesión. A continuación, se desinstalará la aplicación del terminal.
31. En la mayor parte de los casos, el protocolo recomendable será devolver el dispositivo al Administrador o realizar un reseteo a modo fábrica del terminal móvil, generalmente desde Ajustes, Copia de seguridad, Restablecer datos de fábrica (versiones de Android 6 y 7), o en Ajustes, Sistema, Opciones de recuperación, Borrar todos los datos (versiones de Android 8).
32. En caso de no poder resetear el dispositivo, se deben eliminar mediante un explorador de ficheros en el propio dispositivo la carpeta SecureFiles de la carpeta raíz del almacenamiento interno del dispositivo.

## 5.2 DESTRUCCIÓN DEL SERVIDOR IMS

33. Si el servidor IMS debe ser abandonado, tanto de forma permanente como por un periodo de tiempo en el que no puede ser garantizada su seguridad física o lógica, debe aplicarse el procedimiento de borrado de emergencia en cada una de las máquinas del servidor, mediante la ejecución de los scripts IMSZeroing.bat que hayan sido preparados en el momento de la instalación del sistema.
34. Deben realizarse de forma periódica copias de respaldo del servidor IMS para su recuperación ante posible pérdida o daño de datos del mismo, que serán custodiadas siguiendo la normativa aplicable. El periodo para realizar estas copias será definido por el responsable del sistema.

# 6 OPERATIVA ADMINISTRADOR COMSEC

35. El Administrador COMSec se encargará de la gestión de usuarios y del mantenimiento del servidor IMS.

36. Para una completa guía de Administración del IMS véase el documento Ref. [1] IMS_Web_Administrator_Manual_ES_A15_SILODES.

37. El Administrador de Claves se encarga de la gestión de usuarios y claves del sistema COMSec. Para realizar estas tareas, el Administrador de Claves debe disponer de la consola de administración web del IMS (con perfil SuperAdmin).

## 6.1 GENERACIÓN DE OTP

38. El administrador de Claves se encargará de proporcionar las contraseñas OTP a los usuarios del sistema. Este procedimiento se utiliza para la carga inicial de usuarios al sistema o cuando un usuario olvida sus credenciales de acceso. El Administrador decidirá en el momento de la generación del OTP si enviarlo directamente al usuario a través del correo electrónico o mostrarlo por pantalla para hacérselo llegar al destinatario por otros medios.

## 6.2 GESTIÓN DE INCIDENCIAS DE APLICACIÓN.

39. Las aplicaciones COMSec están configuradas para enviar las trazas generadas en caso de errores inesperados. Estas trazas se enviarán por correo electrónico al usuario administrador del IMS. El contenido del mensaje viaja cifrado usando una clave preestablecida que comparten la aplicación COMSec y el Administrador del IMS. El Administrador del IMS debe encargarse de reportar los ficheros de trazas generados directamente a los desarrolladores de la aplicación para subsanar lo más rápido posible las incidencias de aplicación.

## 6.3 GESTIÓN DE CERTIFICADOS

40. El Administrador COMSec se encargará de la gestión de los certificados del IMS. A continuación, identificamos los diferentes certificados que se utilizan en el IMS.

### 6.3.1 CERTIFICADOS PROPIOS

41. Son los certificados con los que se identifica el servidor IMS ante el resto de usuarios. En el establecimiento inicial del enlace TLS, el IMS utiliza este certificado para que se pueda verificar la identidad del IMS. Estos certificados tienen también asociada una clave privada que se guarda en el sistema.

42. En principio, con un solo certificado y su clave privada asociada es suficiente para el correcto funcionamiento del sistema. Adicionalmente, al igual que con los certificados de usuarios, es posible configurar varios certificados propios para el servidor IMS con periodos de validez solapados en el tiempo para tener siempre un certificado válido en

vigor. El certificado usado será el que, siendo válido2, tenga la fecha de caducidad menor.

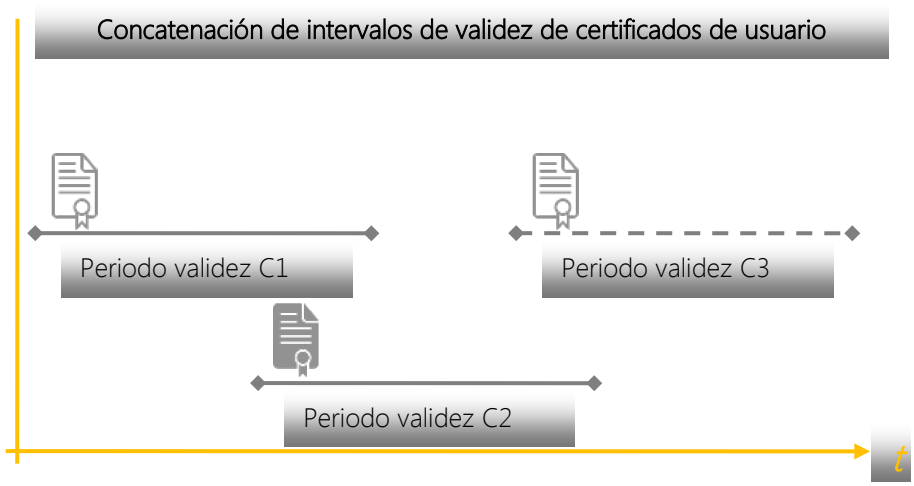


*Figura 3. Ejemplo de intervalos de validez de certificados solapados.*

### 6.3.2 CERTIFICADOS DE CA

43. Son aquellos certificados pertenecientes a entidades de certificación que se utilizan para validar los certificados de cliente que se conectar con el servidor IMS. También se incluyen aquí los certificados de las CAs que forman parte de la cadena de certificación propia.

44. Estos certificados serán necesarios para para establecer relaciones de federación con otros servidores IMS. Mediante los certificados de CAs instalados se validarán los certificados que presentan los IMS federados de otras organizaciones que se conectan nuestro servidor.

## 6.4 GESTIÓN DE USUARIOS

45. El Administrador COMSEC se encargará de la gestión de los usuarios del sistema. Sera el encargado del alta, baja, permisos y visibilidades de los usuarios.

### 6.4.1 PERMISOS DE USUARIO.

46. El sistema COMSec permite asignar de forma individual las operaciones que cada usuario tiene autorización para realizar. Los distintos permisos que se pueden asociar a cada usuario son:

- Llamadas de voz
- Llamadas de vídeo
- Mensajería instantánea (CHAT)
- Archivos adjuntos.
- Llamadas STU (Llamadas a números telefónicos externos a través de centralita)

[2] Ser válido indica que se está en un tiempo actual mayor o igual que el campo *NotBefore* del certificado.

### 6.4.2 VISIBILIDAD ENTRE USUARIOS

47. La relación entre usuarios en el sistema COMSec se organiza a través de visibilidades. El Administrador, para cada usuario, debe seleccionar a que usuarios del sistema puede ver y que usuarios del sistema pueden verlo a él. Las visibilidades pueden ser asimétricas, en este caso sólo el usuario que tiene visibilidad con los demás puede iniciar la comunicación. Para mayor información acerca de este punto, consultar Ref. [1] IMS_Web_Administrator_Manual_ES_A15_SILODES

# 7 GUÍA DE OPERACION APLICACIÓN COMSEC

## 7.1 ARRANCAR COMSEC

48. Para arrancar la aplicación COMSec, pulsar en la pantalla principal del dispositivo sobre el icono COMSec.

49. Se accede a la pantalla de conexión del COMSec donde el usuario debe introducir su nombre de usuario y su contraseña para acceder al sistema.


*Figura 4. Registro IMS*

50. Para poder registrarse, se necesita usuario y contraseña que será suministrado por el Administrador del IMS, encargado de crear usuarios y contraseñas. El usuario y contraseña no está asociado al terminal, sino que es único por persona y podrá iniciarse con el mismo en cualquier dispositivo que disponga de la aplicación COMSec.

51. Pulsar Conectar para registrarse en el IMS una vez se han introducido los datos requeridos.

52. En caso de que fuera necesario realizar modificaciones en la configuración de la conexión, pulsar botón inferior izquierdo del terminal, pulsar Configuración y revisar configuración de los datos de conexión al IMS.

## 7.2 MARCADOR TELEFÓNICO

53. La pantalla Marcador, es la principal del COMSec, donde aparece el teclado telefónico y desde donde se puede realizar llamadas seguras.

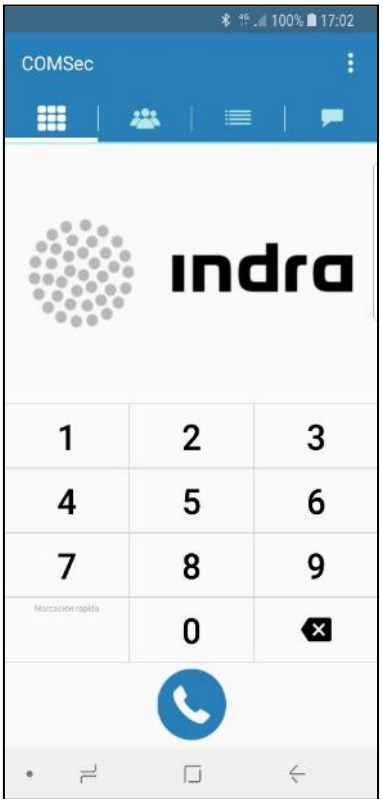


*Figura 5. Pestaña marcador*

54. Para realizar una llamada, se puede pulsar la extensión del usuario a llamar y pulsar la Tecla de Llamada.

55. Una vez se pulse tecla de Llamar aparece una notificación en pantalla "Estableciendo Llamada".

56. Cuando destino acepta la llamada, aparece "Llamada Segura Establecida. Pulsar tecla de Colgar para finalizar la llamada.

57. Pulsando botón de llamar, se accede al histórico de llamadas para poder realizar una re-llamada.

## 7.3 PANTALLA USUARIOS

58. En esta pantalla se muestran los usuarios del sistema COMSec. Está formada por tres sub pestañas:

- Grupos: Grupos de mensajería entre usuarios COMSec
- COMSec: Usuarios del sistema
- Agenda: Contactos personales del terminal, a los que se puede llamar a través de COMSec

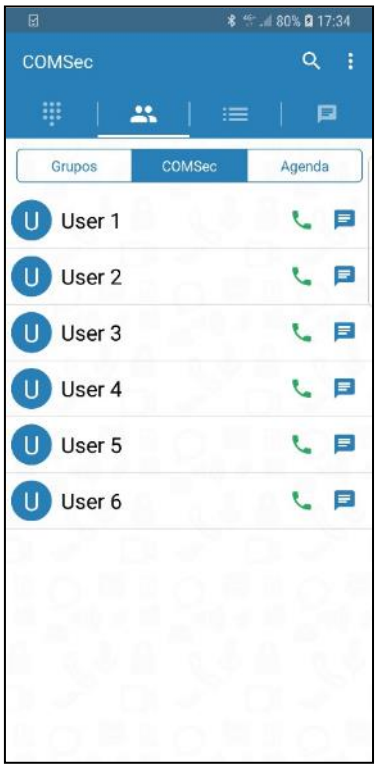


*Figura 6. Pestaña usuarios*

59. Para llamar a un usuario pulse el icono del teléfono.

60. Para enviar un mensaje, pulse el icono a la derecha del teléfono.

## 7.4 INFORMACIÓN DE USUARIO

61. Pulsando sobre cualquier usuario aparecerá información detallada.


*Figura 7. Información de usuario*

62. Aquí se muestra el nombre de usuario, cargo dentro de la administración y extensión.
63. Desde aquí se pueden realizar diferentes acciones contra ese usuario:

- **Llamar:** Llamada segura de voz. Envío y recepción de audio.
- **Enviar Mensaje:** Mensajería instantánea segura.
- **Video Llamada:** Video llamada segura. Se envía y recibe audio y video.
- **Llamada Video TX:** Transmisión segura de video. Se envía audio y video. Solo se recibe audio.

## 7.5 REGISTRO DE LLAMADAS

64. Esta pestaña muestra las llamadas realizadas desde el terminal. Cada llamada viene con un identificador que define el tipo de llamada (recibida, enviada o perdida). Especifica también la extensión de cada usuario y el tiempo desde que se produjo la llamada.

65. Para realizar llamada o enviar un mensaje desde el histórico de llamadas, pulsar en el icono correspondiente que aparece a la derecha de cada registro.


*Figura 8. Registro de llamadas*

66. Pinchando sobre el registro de una llamada se puede obtener información adicional sobre la llamada. Los datos que se muestran son:

- Nombre del usuario
- Extensión telefónica segura
- Tipo de llamada
- Fecha y hora de la llamada
- Duración de la llamada

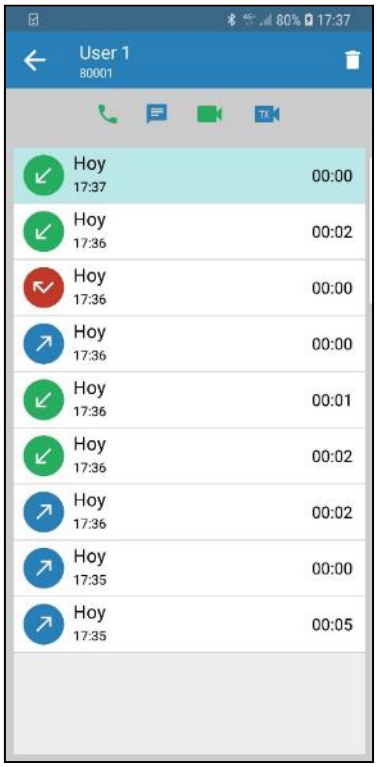


*Figura 9. Detalle de llamada*

## 7.6 MENSAJERÍA SEGURA

67. Desde la pestaña de Mensajes se pueden entrar al histórico de conversaciones de mensajería instantánea.
68. Este menú facilita el rápido acceso a la redacción de los mensajes, a la creación de nuevos grupos de chat y a la carpeta contenedora de los ficheros seguros.
69. En cada conversación de chat se informa si existen mensajes sin leer.
70. En la parte superior de la pantalla se muestra un icono en forma de "bocadillo" donde sin tener el COMSec en primer plano de pantalla, se puede observar que hay mensajes sin leer.
71. Pulsando cualquier conversación se puede continuar enviando mensajes.

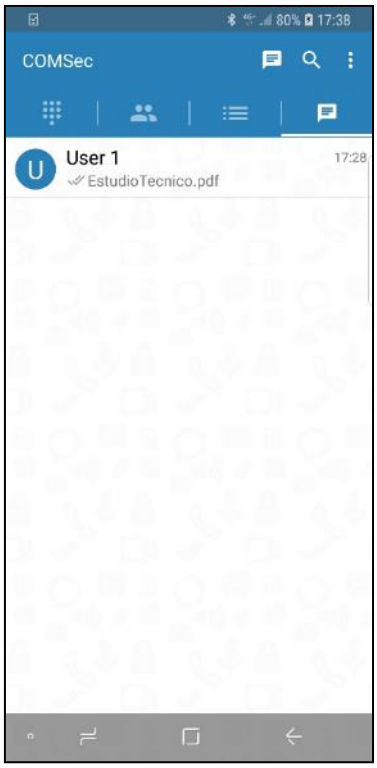


*Figura 10. Mensajería segura*

## 7.7 INTERFAZ MENSAJERÍA

72. En la ventana de chat se pueden enviar y recibir mensajería instantánea.

73. En cada mensaje enviado se puede comprobar si el mensaje ha sido enviado, si ha sido entregado o si ha sido leído, según el icono que acompaña a cada mensaje.

74. Cada mensaje enviado va acompañado de la fecha y hora del envío.

75. Los mensajes enviados se muestran en fondo verde, y los mensajes recibidos se muestran en fondo azul.


*Figura 11. Conversación con usuario*

76. Desde esta pantalla además de mensajes de texto, se puede transmitir al usuario:

- Notas de voz
- Ficheros
- Imágenes
- Información de contacto
- Localización de usuario

## 7.8 MENSAJES DE GRUPO

77. Desde la pestaña de mensajes se pueden crear grupos de mensajería. Un grupo permite comunicarnos con varios usuarios a la vez.

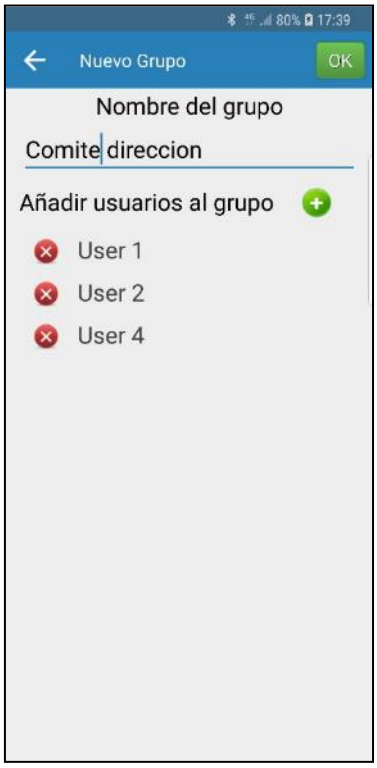


*Figura 12. Mensajes de grupo*

## 7.9 AJUSTES

78. Desde aquí se accede a todos los aspectos de configuración de la aplicación COMSec.

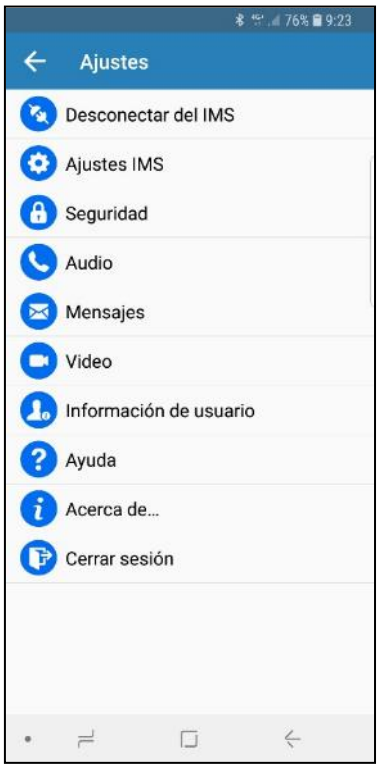


*Figura 13. Ajustes*

79. Para acceder al menú Configuración, pulsar los tres puntos de la esquina superior derecha y pulsar Ajustes. Las diferentes opciones son:

- **Desconectar del IMS** (para posibles actualizaciones de datos de usuarios o forzar una desconexión del IMS sin llegar a cerrar la aplicación).
- **Ajustes IMS**
- **Seguridad**
- **Audio**
- **Mensajes**
- **Video**
- **Información de usuario.** Muestra la extensión asignada al usuario y estadísticas de uso.
- **Ayuda**
- **Comprobar actualizaciones**. Comprueba si existe una versión más actual de la aplicación
- **Acerca de...** Muestra la versión COMSec instalada junto con información de la aplicación.

- **Cerrar sesión**. Cierra la sesión con el IMS. El usuario deberá introducir las credenciales de usuario de nuevo para conectarse con el servidor IMS

### 7.9.1 AJUSTES IMS

80. Desde este menú configuramos los aspectos relacionados con la conexión entre la aplicación y el servidor IMS.

- Opciones avanzadas
- Cierre de conexión con servidor. Esta opción activa el **modo PUSH**, permitiendo al terminal ahorrar batería. La aplicación se conectará al servidor IMS sólo cuando reciba un aviso de mensajes o llamadas a través de un servidor externo. Si el usuario advierte que las notificaciones le llegan tarde, debe desactivar esta opción.
- WiFi limitada, auto-conmutar a 3G. En WiFi donde los FW limiten las conexiones a determinados puertos, cambia a 3G.


*Figura 14. Ajustes IMS*

### 7.9.2 OPCIONES AVANZADAS

81. Desde este menú se pueden configurar opciones relacionadas con la seguridad sobre la interfaz entre la aplicación y el servidor IMS.

- Lanzar aplicación al inicio para que arranque COMSec al encender el terminal
- Inicio sesión automática para recordar usuario y contraseña.
- Recordar nombre usuario para que al abrir la aplicación se muestre el anterior usuario con el que se ha iniciado sesión.


*Figura 15. Opciones avanzadas IMS*

### 7.9.3 SEGURIDAD

82. En esta pestaña encontramos las siguientes opciones:

- **Cambiar contraseña.** Cambia la contraseña de usuario usada para la conexión con el IMS.
- **Código de acceso.** Sirve para proteger la aplicación de uso por terceras personas. Si el terminal lo soporta, puede usarse la autentificación por huella para desbloquear COMSec.
- **Copias de seguridad locales.** Permite generar una copia de seguridad de la Base de Datos local del terminal para importarla desde otro dispositivo.
- **Teclado seguro.** Habilita un teclado que protege sobe escuchas de eventos de teclado por terceros.
- **Permitir capturas de pantalla.**
- **Mostrar código de verificación.**
- **Mostrar logo no corporativo.** Muestra un logo más discreto si activamos esta opción.
- **Reportar incidencias de aplicación.** Informa al administrador del sistema cuando hay un problema con la aplicación. Esta opción ayuda a depurar errores.
- **Certificados de aplicación.** Muestra las CAs de confianza usadas para la conexión con el servidor IMS.

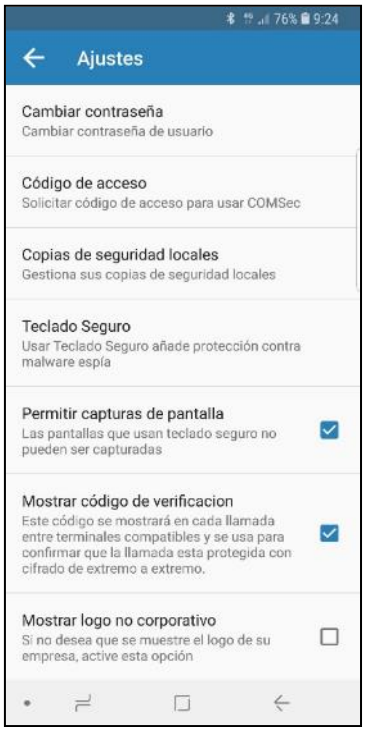


*Figura 16. Opciones de seguridad.*


*Figura 17. Cambio de contraseña.*

### 7.9.4 AUDIO

83. Configuramos aquí todas las opciones relacionadas con las llamadas de voz.


*Figura 18. Ajustes de llamada*

### 7.9.5 MENSAJES

84. Opciones de configuración relacionadas con la mensajería de la aplicación.


*Figura 19. Opciones de mensajes*

## 7.10 DIRECTIVAS DE SEGURIDAD DE USUARIO FINAL COMSEC

85. A continuación, se describen ciertas consideraciones que el usuario final debe tener en cuenta acerca del uso adecuado de la aplicación.

### 7.10.1 CONTRASEÑA DE USUARIO

86. La contraseña de usuario es el mecanismo de autenticación del usuario para poder usar la aplicación. El usuario deberá establecer su contraseña una vez el administrador de Claves le proporcione un OTP para su usuario. La contraseña de usuario debe de ser conocida sólo por el usuario y debe además ser difícil de predecir. Recordar la contraseña es responsabilidad del usuario. Si el usuario olvida su contraseña, deberá solicitarse un nuevo OTP al administrador de Claves del sistema.

87. El usuario puede en cualquier momento cambiar su contraseña, para ello debe acceder al menú de aplicación: Ajustes -> Seguridad -> Cambiar Contraseña.

### 7.10.2 LLAMADAS EXTREMO A EXTREMO

88. Las claves de llamada entre usuarios del sistema se negocian extremo a extremo. Una vez establecida la llamada aparecerá en pantalla un código de verificación de cuatro dígitos. Este código se proporciona para comprobar que la llamada no está

comprometida por un ataque de hombre en medio (MitM). El código puede ser transmitido al otro usuario por el canal de voz y debe coincidir con el código mostrado en la pantalla remota. Si los códigos difieren se debe abandonar la llamada inmediatamente como medida preventiva frente a un posible ataque y deberá informarse al administrador del sistema lo antes posible.


*Figura 20. Código de verificación de llamada*

### 7.10.3 INICIO DE SESIÓN AUTOMÁTICA

89. Esta opción permite iniciar la aplicación sin introducir la contraseña de usuario. Si bien facilita el acceso al sistema, con esta opción activada se abre la puerta a terceros para usar la aplicación sin una autentificación previa.

90. Esta opción aparece en Ajustes -> Ajustes IMS -> Opciones avanzadas -> Inicio sesión automática.

### 7.10.4 TECLADO SEGURO

91. La aplicación COMSec incorpora un teclado seguro para prevenir la captura de eventos de teclado por aplicaciones de terceros. Para utilizar este teclado seguro, el usuario necesita conceder a la aplicación el permiso especial: Aplicaciones que se pueden mostrar encima. El teclado seguro se usa automáticamente en todas aquellas pantallas que procesen información sensible, como nombres de usuarios, contraseñas, etc. Opcionalmente el usuario puede activar este teclado para la redacción de mensajes de texto.

### 7.10.5 CÓDIGO DE ACCESO

92. COMSec puede utilizar opcionalmente un código de acceso para impedir el uso de la aplicación por terceros. Adicionalmente se puede usar la huella digital, si el dispositivo lo permite, para proteger la aplicación.

93. Si el usuario se olvida del código de acceso podrá usar su contraseña de usuario COMSec como alternativa para resetear su código de acceso.

94. Se recomienda encarecidamente al usuario activar esta funcionalidad desde el menú Seguridad -> Código de acceso.

### 7.10.6 CAPTURAS DE PANTALLA

95. Por defecto la aplicación no permite capturas de pantalla. Se puede modificar este comportamiento mediante la opción: Ajustes -> Seguridad -> Permitir capturas de pantalla. No se recomienda activar esta opción.

### 7.10.7 MENSAJES CON ACUSE DE RECIBO Y AUTOBORRADO

96. El sistema proporciona la funcionalidad de mensajería entre usuarios. Se pueden activar las opciones de Acuse de recibo y Auto borrado al enviar un mensaje.

    - **Acuse de recibo**: Da información al usuario de cuando el extremo remoto lee el mensaje.
    - **Auto borrado**: Los mensajes se eliminan de la aplicación de forma automática después de que el extremo remoto los haya leído.

97. Se recomienda usar la opción de auto borrado para transmitir información muy sensible entre usuarios de forma que se minimicen riesgos.

### 7.10.8 COPIAS DE SEGURIDAD DE BASE DE DATOS DE USUARIO

98. La aplicación COMSec permite hacer una copia de seguridad de la base de datos y almacenarla en el almacenamiento del dispositivo. Esta copia permanecerá cifrada con una contraseña que sólo debe conocer el propio usuario.

99. La gestión de copias de seguridad se realiza desde el menú Ajustes -> Seguridad -> Copias de seguridad locales.

100. Esta funcionalidad permite transportar la información de usuario de un dispositivo a otro. Para transportar una copia de seguridad entre terminales se debe trasladar el fichero generado en el directorio SecureFiles/Backups desde el dispositivo original al nuevo dispositivo. Una vez se disponga de la copia de seguridad, se debe acceder en la aplicación a la opción Restaurar copia de seguridad y seleccionar la copia de seguridad que deseemos restaurar. Esta acción reemplaza el contenido actual de la aplicación por el de la copia de seguridad.

# 8 REFERENCIAS

[1] IMS_Web_Administrator_Manual_ES_A15_SILODES.DOCX
[2] CCN-STIC 521 Configuración segura de Windows Server 2008 R2
[3] CCN-STIC 105 Catálogo de productos de seguridad TIC
[4] CCN-STIC 496 Sistemas de Comunicaciones Móviles Seguras