

EL CENTRO CRIPTOLÓGICO NACIONAL ACREDITA LAS CAPACIDADES FRENTE A LA COMPUTACIÓN CUÁNTICA DE LA SOLUCIÓN DE INDRA GROUP PARA COMUNICACIONES MÓVILES SEGURAS, COMSEC

- **COMSec se consolida como la única solución de su clase en España avalada por este organismo para comunicaciones móviles seguras con capacidad *quantum resistant*, ofreciendo una protección integral tanto ante amenazas presentes como futuras**
- **La nueva versión 5.1 de COMSec incorpora tecnologías de criptografía post-cuántica (PQC) para anticiparse a las futuras amenazas cuánticas, como la “*harvest now, decrypt later*” mediante la cual los datos almacenados en la actualidad puedan ser descifrados en el futuro**

Madrid, 14 de julio de 2026. – La nueva actualización de la solución de comunicaciones móviles seguras de Indra, COMSec, ha sido incorporada al *Catálogo de Productos de Seguridad TIC (CPSTIC)* del Centro Criptológico Nacional (CCN), como solución cualificada y apta para su uso en sistemas del Esquema Nacional de Seguridad (ENS) de nivel Alto y aprobada para Difusión Limitada. Se sitúa, así como la única solución de su clase avalada por este organismo para comunicaciones móviles seguras con capacidad *quantum resistant* en España, ofreciendo una protección integral tanto ante amenazas presentes como futuras.

La nueva actualización de COMSec, la versión 5.1, incorpora tecnologías de criptografía postcuántica (PQC), un avance decisivo para anticiparse al riesgo que pueden llegar a suponer los futuros ordenadores cuánticos y la amenaza conocida como “*harvest now, decrypt later*”, por la cual la información interceptada hoy podría ser descifrada dentro de unos años.

Esta mejora se alinea con las recomendaciones del CCN a la transición postcuántica segura recogida en la guía CCN-TEC-009, la guía CCN-STIC 221 sobre los algoritmos criptográficos autorizados y los calendarios oficiales que marcan la transición hacia sistemas híbridos que combinen criptografía clásica y postcuántica. Además, Indra ha sido pionera en la incorporación de este tipo de tecnología tanto en España como a nivel internacional, incluyendo el proceso de certificación criptológica MEMeC.

El sistema COMSec permite transmitir voz y datos de forma segura utilizando las redes de cualquier operador comercial. Se implementa sobre una gran variedad de teléfonos móviles comerciales sobre los sistemas operativos más utilizados. Las comunicaciones se basan en el envío de paquetes IP con protocolos propietarios y cifrados, lo que impide su rastreo. El sistema consta de una aplicación instalada en el dispositivo del usuario y en un operador virtual (IMS) que los gestiona.

COMSec mantiene su diseño security-by-design y su cifrado de extremo a extremo (E2EE) para voz, mensajería instantánea, videollamadas y transferencia de datos, integrándose en arquitecturas locales *on-premise* y entornos altamente controlados. Las nuevas capacidades PQC se han incorporado sin afectar a la experiencia de usuario, manteniendo la robustez y la baja latencia que caracterizan al producto.

“Con esta actualización en el Catálogo de Productos de Seguridad TIC, Indra refuerza su liderazgo como desarrollador nacional de soluciones avanzadas de comunicaciones seguras y como referente en criptografía postcuántica, en estrecha colaboración con el Centro Criptológico Nacional. Reforzamos también nuestro compromiso con la protección de las comunicaciones y la información sensible en organismos gubernamentales y entidades estratégicas de nuestro país”, subraya Francisco Jiménez, director de Sistemas de Comunicaciones Seguras de Indra.

Indra Group sigue reforzando su liderazgo en tecnologías cuánticas, con capacidades en comunicaciones, pero también en sensórica avanzada, gestión de claves y computación. Lidera la implementación de la red nacional de comunicaciones cuánticas que se integrará en la red europea de comunicaciones cuánticas EuroQCI, así como el proyecto IberianQCI, a través de Indra Space, que representa el segmento del sudoeste de Europa de la futura red europea e interconecta con comunicaciones terrestres y satelitales las infraestructuras de España y Portugal.

Indra Group colabora con las universidades, centros tecnológicos, empresas y startups especializadas en tecnologías cuánticas nacionales y europeas para generar un ecosistema tecnológico de referencia internacional.

Acerca de Indra Group

Indra Group (www.indracompany.com) es la multinacional española de referencia y una de las principales compañías de Europa en defensa y digitalización avanzada. Tiene una posición de liderazgo en los negocios de defensa, espacio, gestión de tráfico aéreo, movilidad y tecnologías transformadoras, a través de Minsait, e integra en IndraMind sus capacidades de IA soberana, ciberseguridad y ciberdefensa. Indra Group impulsa un futuro más seguro y conectado a través de soluciones innovadoras, relaciones de confianza y el mejor talento. La sostenibilidad forma parte de su estrategia y de su cultura, para dar respuesta a los retos sociales y ambientales presentes y futuros. A cierre del ejercicio 2025, Indra Group tuvo unos ingresos de 5.457 millones de euros, presencia local en 46 países y operaciones comerciales en más de 140 países.

Contacto de Comunicación

Toñi García Carballal
magcarballal@indra.es
+34 648 10 29 48