Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Enrique Belda Esplugues
Doctor Ingeniero por la U. Politécnica de Valencia.
Subdirector General de Sistemas de Información y Comunicaciones para la Seguridad y Director del Centro Tecnológico de Seguridad.
Secretaría de Estado de Seguridad
Ministerio del Interior.

LA TRANSFORMACIÓN DIGITAL EN EL MINISTERIO DEL INTERIOR. RETOS DE FUTURO. EL CENTRO TECNOLÓGICO DE SEGURIDAD (CETSE)

LA TRANSFORMACIÓN DIGITAL EN EL MINISTERIO DEL INTERIOR RETOS DE FUTURO EL CENTRO TECNOLÓGICO DE SEGURIDAD (CETSE)

Resumen: Como parte de las funciones encomendadas a la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS) de la Secretaría de Estado de Seguridad del Ministerio del Interior, se encuentra la dirección del Centro Tecnológico de Seguridad (CETSE), desde el que se impulsan múltiples iniciativas tecnológicas y de transformación digital al objeto de servir como herramientas de apoyo a la misión ejercida por las Fuerzas y Cuerpos de Seguridad del Estado de salvaguarda de los derechos y libertades de los ciudadanos, así como al propio Ministerio del Interior en el cumplimiento de sus funciones. El CETSE se ha convertido en un Centro de referencia digital, idóneo para atraer la excelencia tecnológica y dotar al Ministerio del Interior de capacidad de innovación en el ámbito de las tecnologías para la Seguridad. Hoy, el Centro Tecnológico de la Seguridad (CETSE) es una realidad que gestiona más de 100 proyectos. Así pues, desde este Centro, podemos identificar sectores industriales, investigar tendencias de futuro y motivar a los interesados hacia acciones tecnológicas innovadoras.

Abstract: As a part of the functions entrusted to the Deputy Direction General of Communication and Information Systems for Security (SGSICS) of the Secretary of State for Security of the Ministry of the Interior, there is the direction of the Security Technology Centre (CETSE), from which multiple technological and digital transformation initiatives are promoted in order to serve as support tools for the mission carried out by the State Security Corps and Forces to safeguard the rights and freedoms of citizens, as well as the Ministry of the Interior itself in the fulfilment of their functions. The CETSE has become a digital reference centre, ideal for attracting technological excellence and providing the Ministry of the Interior with the capacity for innovation in the field of security technologies. Today, the Security Technology Centre (CETSE) is a reality that manages more than 100 projects. Thus, from this Centre, we can identify industrial sectors, investigate future trends and motivate stakeholders towards innovative technological actions.

Palabras clave: Sistemas de Información y Comunicaciones. Transformación Digital. Seguridad Pública. Centro Tecnológico.

Keywords: Information and Communication Systems. Digital Transformation. Public Security. Tecnnology Centre.

1.- INTRODUCCIÓN

Durante la última década, la irrupción de las Tecnologías de la Información en el mundo de la delincuencia grave y organizada (como el tráfico de seres humanos y drogas) y al mismo tiempo su uso por terroristas y organizaciones terroristas, hace necesario dotar a las Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE) de instrumentos capaces de luchar contra esa realidad con el claro objetivo de aumentar la seguridad, sin la cual las personas no pueden ejercer su libertad y los derechos individuales de manera efectiva.

En ese sentido, la dimensión de nuestras FFCCSE hace necesario planificar con gran precisión la adquisición del conjunto de sistemas tecnológicos de información y comunicaciones que les sirvan como apoyo a la consecución de sus objetivos, procurando su presente y futura sostenibilidad, siendo la única vía que lo permite la planificación y gestión conjunta, escalable e interoperable de todas y cada una de las soluciones necesarias, posibilitando disponer en todo momento de las últimas actualizaciones de cada uno de los sistemas gestionados.

Con ese fin surgió en febrero de 2013 la creación del concepto de Centro Tecnológico y así, la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS) de la Secretaría de Estado de Seguridad, puso en marcha el proyecto del Centro Tecnológico para la Seguridad (CETSE) que tomó forma en abril de 2016 en las nuevas instalaciones de El Pardo (Madrid). Hoy se ubican en las mencionadas dependencias tres unidades de la Secretaria de Estado de Seguridad: la propia SGSICS, el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC) y la Oficina de Coordinación Cibernética (OCC).

Figura 1. Centro Tecnológico de Seguridad (El Pardo). Fuente: elaboración propia.

De forma particular, la SGSICS tiene asignadas el conjunto de funciones encaminadas a la planificación, propuesta y coordinación del desarrollo e implantación de bases de datos, sistemas de información y sistemas de comunicaciones de utilización conjunta o compartida por las FFCCSE en base a las necesidades de las mismas, al objeto de dotarles de las capacidades y herramientas que les permitan ejercer su labor de salvaguarda de los derechos y libertades de los ciudadanos en los distintos ámbitos de seguridad (prevención del delito en sus diversas naturalezas, investigación, reacción y gestión de crisis, etc.) de una manera más eficiente, eficaz y adaptada a los retos tecnológicos de futuro.

2.- PROYECTOS DESTACADOS

Poniendo el foco en los últimos años, entre las líneas estratégicas llevadas a cabo por la SGSICS cabe destacar la modernización y evolución de los siguientes proyectos:

2.1.- Ámbito telecomunicaciones

Desde la SGSICS se gestiona la modernización del Sistema de Radiocomunicaciones Digitales de Emergencia del Estado (SIRDEE) que actualmente dota de capacidades para la gestión de comunicaciones seguras de voz y datos a las FFCCSE y otros organismos, como la Unidad Militar de Emergencias (UME), policías municipales y servicios de emergencia y de gestión de crisis, a través de una red propia de comunicaciones con más de 70.000 terminales, preparándolo para la siguiente evolución en las Tecnologías de las Comunicaciones, la Tecnología LTE, cuya fecha prevista de implantación progresiva se ha fijado para 2025.

Así mismo, se ha implementado un modelo de servicio para la gestión del Sistema de Interceptación Legal de las Telecomunicaciones y Conservación de Datos, cuya finalidad es la recepción y registro centralizado de las comunicaciones electrónicas interceptadas por orden judicial para su posterior presentación por parte de la Policía Nacional o Guardia Civil como evidencia en procesos judiciales relacionados con investigaciones en la lucha contra el terrorismo, tráfico de drogas y delincuencia organizada.

2.2.- Fronteras inteligentes

El Proyecto de Fronteras Inteligentes (Smart Borders) parte de una iniciativa europea con el objetivo gestionar de una manera integral las fronteras aéreas, marítimas y terrestres. En este sentido, desde la SGSICS se lideró el lanzamiento de la implementación del Sistema Automatizado de Control de Fronteras (Automated Border Control, ABC System) que, basándose en la identificación biométrica y documental de los viajeros, permite agilizar e implementar un cruce desasistido de fronteras, así como la implantación de Centros de Control y Coordinación de Puestos Fronterizos como el situado en las dependencias de la Comisaría General de Extranjería y Fronteras de Policía Nacional en Madrid o en el Puerto de Algeciras.

Figura 2. Sistema ABC en el aeropuerto de El Prat (Barcelona). Fuente: elaboración propia.

Figura 3. Centro Nacional de Coordinación de Puestos Fronterizos (Madrid). Fuente: elaboración propia.

Por otra parte, mediante el Reglamento (UE) 2017/2226, aprobado en noviembre de 2017, se decidió establecer un nuevo Sistema de Entradas y Salidas (Entry Exit System, EES) para registrar la información sobre la entrada, la salida y la denegación de entrada de los ciudadanos de terceros países (Third Country Nationals, TCN) que cruzan las fronteras exteriores de los Estados Miembros de la UE dentro del espacio Schengen.

EES será un sistema informático automatizado para registrar a los viajeros de terceros países, tanto titulares de visados como viajeros exentos de visado, cada vez que crucen una frontera exterior de la UE. El sistema registrará datos como el nombre de la persona, tipo de documento de viaje, datos biométricos (huellas dactilares e imágenes faciales capturadas) y la fecha y lugar de entrada y salida, con pleno respeto a los derechos fundamentales y a la protección de datos. El Sistema EES también registrará las denegaciones de entrada a ciudadanos de terceros países y sustituirá al actual sistema de sellado manual de pasaportes.

Este sistema forma parte del paquete de Fronteras Inteligentes de la Unión Europea (UE) y, junto con otros sistemas nuevos o revisados (ETIAS, SIS, VIS, etc.), conformará un primer bloque de construcción de la nueva arquitectura de los sistemas informáticos interoperables de la UE, bajo la responsabilidad de la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA). Con la entrada en funcionamiento del EES, se contribuirá a:

- Reforzar la seguridad interna y la lucha contra el terrorismo y el crimen transfronterizo, así como prevenir la migración irregular (ilegal).
- Identificar con mayor eficacia a los viajeros que exceden el tiempo de estancia máxima, así como los casos de fraude de documentos e identidad.
- Facilitar el cruce de fronteras a los TCN de buena fe a través de un uso más amplio de los controles fronterizos automatizados, más rápidos y cómodos para el viajero.

A nivel nacional, el Ministerio del Interior, a través de la SGSICS y Policía Nacional, ha planteado un ambicioso proyecto que actualmente se encuentra en desarrollo para la implementación por fases del EES. Esto incluye la implementación del sistema central nacional EES, puestos de control manual para su utilización por parte de los agentes de fronteras, así como de equipamiento para el control automatizado en puntos de control fronterizos terrestres, aeroportuarios y portuarios, en estrecha colaboración con AENA, Puertos del Estado y las Autoridades Portuarias.

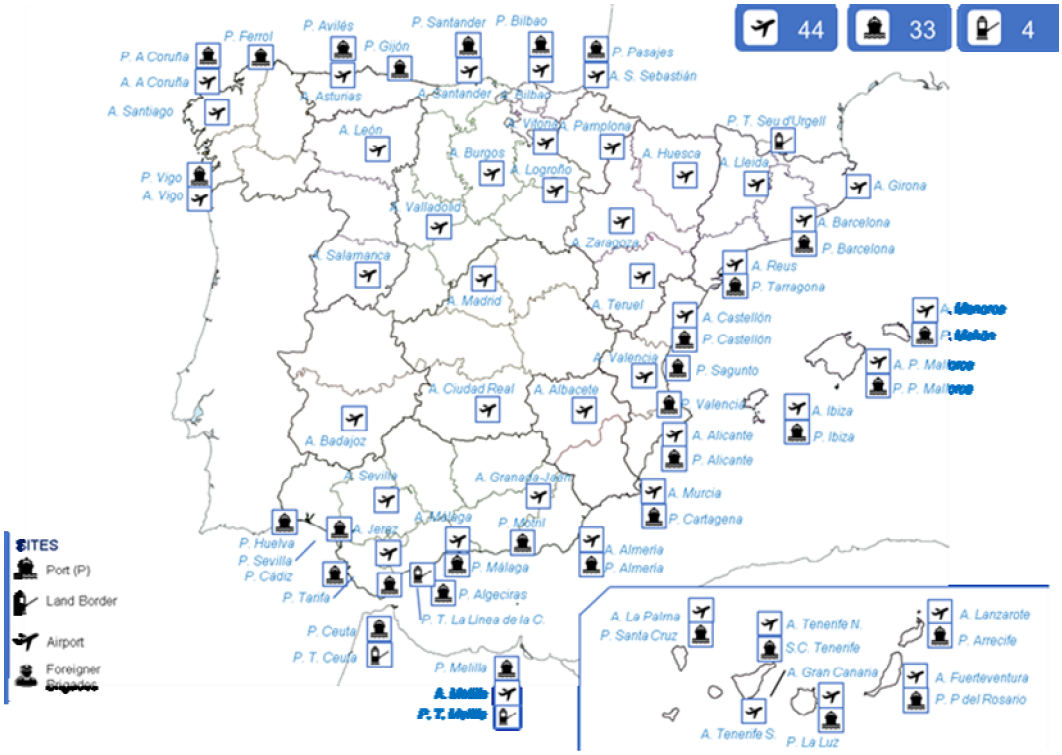

Figura 4. Distribución geográfica de los puntos fronterizos dónde se prevé desplegar equipamiento de EES. Fuente: elaboración propia.

En el mismo objetivo de seguir reforzando la seguridad en las fronteras exteriores del espacio Schengen, mediante el Reglamento (UE) 2018/1240, de 12 de septiembre de 2018, se establece un Sistema Europeo de Información y Autorización de Viajes (European Travel Information and Authorization System, ETIAS) y por el que se modifican los Reglamentos (UE) n.o 1077/2011, (UE) n.o 515/2014, (UE) 2016/399, (UE) 2016/1624 y (UE) 2017/2226.

ETIAS forma parte del paquete de fronteras inteligentes de la UE y está específicamente destinado a los nacionales de terceros países exentos de la obligación de visado para cruzar las fronteras, permitiendo evaluar si la presencia de dichos nacionales de terceros países en el territorio de los Estados Miembros supone un riesgo para la seguridad, un riesgo de inmigración ilegal o un riesgo elevado de epidemia. A tal efecto se establecen una autorización de viaje y las condiciones y procedimientos para expedirla o denegarla. Con la implantación del ETIAS, se controlará la validez de la autorización de viaje que los nacionales de terceros países habrán debido solicitar con anterioridad a su viaje. Los principales objetivos de ETIAS, son:

- Contribuir a un alto nivel de seguridad aportando una rigurosa evaluación del riesgo para la seguridad que presentan los solicitantes, antes de su llegada a los pasos fronterizos exteriores, con el fin de determinar si existen indicios concretos o motivos razonables basados en indicios concretos para concluir que la presencia de la persona en el territorio de los Estados Miembros supone un riesgo para la seguridad;
- Contribuir a la prevención de la inmigración ilegal aportando una evaluación del riesgo de inmigración ilegal de los solicitantes antes de su llegada a los pasos fronterizos exteriores;

- Contribuir a la protección de la salud pública aportando una evaluación de si el solicitante supone un riesgo elevado de epidemia antes de su llegada a los pasos fronterizos exteriores;
- Aumentar la eficacia de las inspecciones fronterizas;
- Apoyar los objetivos del SIS relacionados con descripciones sobre nacionales de terceros países que sean objeto de una prohibición de entrada y estancia, sobre personas buscadas para su detención a efectos de entrega o extradición, sobre personas desaparecidas, sobre personas en búsqueda para cooperar en un proceso judicial y sobre personas a efectos de controles discretos o controles específicos;
- Contribuir a la prevención, detección e investigación de delitos de terrorismo o de otros delitos graves.
- Favorecer la entrada y salida para los viajes con carácter de negocios e impulso de la economía.

Con la implantación nacional de ETIAS, que actualmente se encuentra en desarrollo bajo la dirección de la SGSICS y Policía Nacional, se modernizarán las capacidades tecnológicas para los funcionarios encargados del control de fronteras y para los ciudadanos de terceros países. Dichas capacidades incluirán los mecanismos necesarios para la validación de la autorización de viaje ETIAS aportada por el TCN, complementando así los controles realizados gracias al desarrollo del sistema EES.

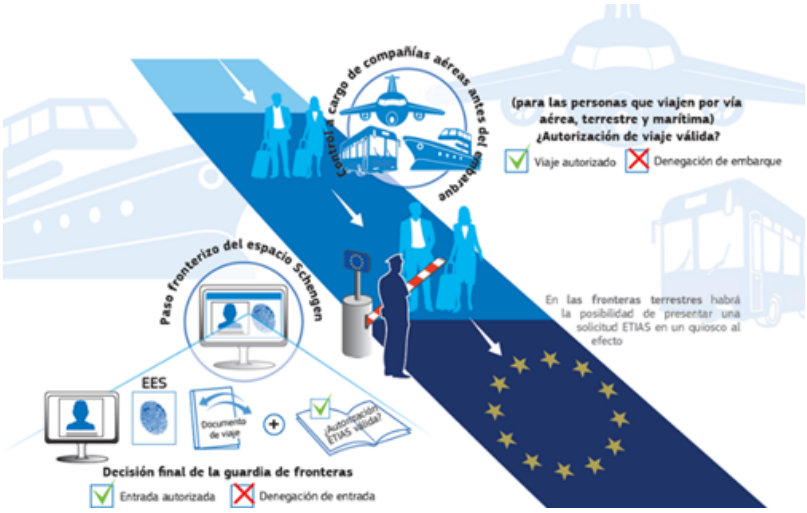

Figura 5. Visión general del sistema ETIAS. Fuente: eu-LISA.

2.3.- Otros sistemas europeos

El pasado 7 de marzo entró en funcionamiento el Sistema de Información de Schengen (Schengen Information System, SIS) recast. El sistema SIS, responsabilidad de la SGSICS a nivel nacional, y cuyos usuarios incluyen a Policía Nacional, Guardia Civil y Fuerzas y Cuerpos de Seguridad autonómicos, es el mayor sistema de intercambio de información para la seguridad y la gestión de fronteras en Europa, así como para la cooperación policial. Proporciona información sobre personas buscadas o desaparecidas, nacionales de terceros países sin derecho legal a permanecer en la Unión y objetos

perdidos o robados (por ejemplo, automóviles, armas de fuego, barcos y documentos de identidad).

El SIS recast se ha mejorado para incluir nuevas categorías de alertas, datos biométricos como huellas palmares, huellas dactilares y registros de ADN de personas desaparecidas y herramientas adicionales para combatir el crimen y el terrorismo. La actualización es importante ya que también permitirá introducir alertas preventivas para proteger a las personas vulnerables y determinar la migración irregular. Estas actualizaciones tienen como objetivo proporcionar a las autoridades nacionales información más completa y fiable para mejorar la seguridad y la gestión de fronteras en Europa. Las características mejoradas incluyen:

- Mayor intercambio de información y cooperación: se compartirán nuevas categorías de alertas y más datos a través del SIS, lo que garantizará que las autoridades nacionales dispongan de información más completa y confiable. Se han introducido normas más claras y estructuras mejoradas para el intercambio de información a través de los puntos de contacto nacionales (oficinas SIRENE).
- Nuevas posibilidades para localizar e identificar a las personas buscadas y reforzar los controles en las fronteras exteriores: además de fotografías y huellas dactilares, el SIS contendrá nuevos tipos de datos biométricos (como huellas palmares, huellas dactilares y marcas palmares, así como registros de ADN, pero solo en relación con personas desaparecidas).
- Herramientas adicionales para combatir la delincuencia y el terrorismo: las nuevas alertas sobre controles de investigación permitirán a las autoridades nacionales recopilar información específica sobre sospechosos de delitos graves o terrorismo.
- Habrá alertas sobre “personas desconocidas buscadas”, que contengan solo las huellas de los perpetradores desconocidos que se descubran en las escenas de delitos terroristas o delitos graves.
- Nuevas funcionalidades para proteger a personas desaparecidas y vulnerables: Las autoridades nacionales podrán emitir alertas preventivas en el sistema para proteger a ciertas categorías de personas vulnerables (niños en riesgo de secuestro o posibles víctimas de terrorismo, trata de seres humanos, violencia de género, o conflictos armados/hostilidades), además de las alertas existentes sobre personas desaparecidas.
- Mejoras para prevenir y determinar la migración irregular: Las decisiones de retorno serán parte de la información compartida en el sistema para mejorar la aplicación efectiva de estas decisiones.
- Uso mejorado del SIS por parte de las agencias de la UE: Europol y las autoridades nacionales de inmigración ahora tienen acceso a todas las categorías de alerta en el SIS. Los equipos operativos de la Agencia Europea de la Guardia de Fronteras y Costas (Frontex) han obtenido acceso al SIS.

Para dar consistencia y obtener el máximo rendimiento de los distintos sistemas desarrollados, desde la Comisión Europea se está desarrollando el proyecto de *Interoperabilidad.* En términos generales, se considera como la capacidad de los sistemas de información para intercambiar datos y permitir compartir información, en el caso que nos ocupa, tanto para una gestión eficaz de la seguridad de las fronteras como la seguridad interior de la Unión. Se basa en la gestión y uso de sistemas y bases de datos de grandes sistemas de información europeos centralizados.

Entre los mencionados sistemas figuran los ya existentes: Sistema de Información Schengen (SIS), Eurodac y sistema de visados (VIS), así como los sistemas actualmente en desarrollo, implantación y entrada en operación próxima:

- ECRIS-TCN: Sistema centralizado con los datos necesarios para identificar a nacionales de terceros países con información relativa sanciones penales.
- EES: Sistema para registrar a los viajeros de terceros países, tanto a los titulares de visados de corta duración como a los exentos de visado, cada vez que crucen –entrada o salida- una frontera exterior de la UE.
- ETIAS: Sistema para los ciudadanos de países que actualmente están exentos de visa para visitar el Espacio Schengen, que deseen viajar a Europa para hacer turismo, por tránsito o por negocios.

Siendo la interoperabilidad entre ellos un requisito clave, se han incorporado cuatro elementos básicos que lo hacen posible:

- ESP (European Search Portal): portal europeo de búsqueda que permitirá a los usuarios autorizados realizar una búsqueda única en todos los sistemas mencionados anteriormente y recibir resultados de todos los sistemas a los que estén autorizados a acceder.
- SBMS (Shared Biometric Matching Service): repositorio compartido por todos los sistemas que recogen biométricos que permitirá a los usuarios buscar y cruzar datos biométricos de forma conjunta.
- CIR (Common Identity Repository): repositorio común de identidades que permitirá la información biográfica de los ciudadanos extracomunitarios. Almacenará los datos biográficos de todos los sistemas a excepción del SIS.
- MID (Multiple-Identity Detector): sistema para la detección de identidades múltiples con un doble objetivo de garantizar la correcta identificación de personas de buena fe, así como combatir el fraude de identidad.

Con todos los sistemas interoperables y con una gestión y uso eficaz de los mismos, el objetivo es conseguir una mejora en la gestión de la seguridad, las fronteras y la migración, dando solución a las deficiencias estructurales y compartir la información que actualmente está en “silos”, mejorando las deficiencias que obstaculizan la labor de las autoridades nacionales y garantizar que los policías, tanto de fronteras como seguridad ciudadana, las autoridades aduaneras y las autoridades judiciales tengan a su disposición la información necesaria para realizar su trabajo de forma eficiente y eficaz.

Finalmente, desde la SGSICS se continúa trabajando en la actualización continua del Sistema de Registro de Nombres de Pasajeros (PNR) o Passenger Name Record, que permite la recolección, análisis y establecimiento de relaciones y patrones de información relativa a los pasajeros de vuelos, como prevención de acciones terroristas y de crimen

organizado en nuestras fronteras.

2.4.- Biometría

En este ámbito destaca la actualización del proyecto ABIS, Automatic Biometric Identification System (antiguo SAID – Sistema Automático de Identificación Dactilar-, iniciado en 2007), donde se graban las huellas latentes recogidas en los escenarios de los delitos, así como las dactilares de los detenidos reseñados. Durante el año 2023, ABIS almacenará también imágenes faciales de detenidos, para el desarrollo de investigaciones cuando existan imágenes o videos en donde se hayan captado ilícitos penales.

La Policía Nacional, la Guardia Civil, los Mossos d'Esquadra y la Policía Foral de Navarra comparten esta base de datos que gestiona y coordina la SGSICS, así como la información relacionada existente en las respectivas bases de datos delincuenciales. La Ertzaintza tiene su propio sistema, que desde primeros del año 2015 intercambia datos con el sistema Central.

Estas huellas dactilares almacenadas en España son intercambiadas también dentro del marco del Tratado de Prüm con 21 países europeos con la misma finalidad que los perfiles genéticos.

2.5.- Drones/antidrones

Desde la SGSICS se gestiona el desarrollo del Sistema SIGLO-CD. La mejor forma de describirlo es desglosando sus siglas, Sistema Global Contra Drones, es decir, sistema integrado por diferentes soluciones interoperables, de forma independiente del fabricante, para detectar, identificar, monitorizar y en su caso neutralizar la mayoría de los drones comerciales del mercado.

Basándose en la arquitectura cliente-servidor y huyendo de soluciones propietarias o 'stand-alone', se está creando una red nacional de sistemas de detección y neutralización, gestionado desde un Centro de Mando y Control, que permitirá operar dependiendo de los permisos que se tengan asignados.

Desde la SGSICS se inició el proyecto, tras resolución de la Secretaría de Estado de Seguridad, en el año 2019, para proteger las más altas Instituciones de Estado. A día de hoy el sistema se encuentra en su Fase 1 y detecta sobre el casco urbano de Madrid y de Valencia, siendo capaz de neutralizar drones comerciales en caso de acercarse a determinadas zonas de especial protección. Como referencia, solo en el año 2022, se detectaron 14.000 drones comerciales volando sobre el casco urbano de Madrid.

La siguiente fase del proyecto, actualmente en licitación, se ejecutará durante los años 2023 al 2025. Durante este periodo se desplegarán un total de 32 antenas fijas de detección de las cuales 15, además, irán acompañadas de capacidad de neutralización, junto con 86 maletas de detección portátil y otras 15 de neutralización, también portátiles. Con todo ello se pretende cubrir las ciudades más pobladas del territorio nacional, aumentando la red en siguientes fases.

Actualmente son usuarios del sistema SIGLO-CD, Policía Nacional, Guardia Civil, Servicio de Seguridad de Casa Real, Servicio de Seguridad de Presidencia del Gobierno

y Ministerio de Defensa. Igualmente existe un convenio de colaboración con LaLiga de Fútbol Profesional.

Por otro lado, se siguen analizando el modo de funcionamiento de los drones comerciales que salen al mercado y las posibles soluciones para su detección y, en su caso, neutralización.

2.6.- Plataformas en movilidad

En este ámbito, la plataforma **AlertCops** ha marcado un hito en la prestación de servicios públicos de seguridad ciudadana y constituye un canal innovador para interaccionar con las FFCCSE (canal de comunicación directa Ciudadano-FFCCSE). Gracias a las capacidades de las que hoy en día disponen los smartphones, ha permitido mejorar, tanto la eficacia de la respuesta policial para los ciudadanos, como la colaboración para comunicar situaciones de riesgo.

AlertCops, desarrollado desde la SGSICS, proporciona un servicio público integral y universal de seguridad ciudadana, a través de una aplicación (APP), que se terminó de desplegar a principios del año 2015. Es un canal directo, discreto, eficaz y complementario a los existentes, para comunicar a las FFCCSE una situación de riesgo de la que se es víctima o testigo. Las características clave de AlertCops son:

- Permite llamadas y alertas geo posicionadas para una atención de forma inmediata.
- Habilita un chat directo (tipo WhatsApp) con el centro de atención de las Fuerzas y Cuerpos de Seguridad del Estado más cercano y posibilita el intercambio de fotos y videos.
- Está integrado en la infraestructura existente y no afecta a los protocolos de actuación de las FFCCSE.
- Todo el servicio se presta y se mantiene desde la propia infraestructura tecnológica de la Secretaria de Estado de Seguridad y el 100% de la propiedad del desarrollo y de los componentes que lo forman es del Ministerio del Interior.

Desde su despliegue hasta la fecha, se han ido incorporando muchas más funcionalidades, por peticiones de los ciudadanos, de los grupos de trabajo de las FFCCSE y por parte de agencias públicas (Protección Civil, Sanidad, etc.). Las más significativas son:

- Envío de avisos de seguridad o de colaboración a determinadas zonas.
- Incremento de la presencia en colectivos con nuevas tipologías de alertas: Violencia de género, personas sordas, delitos de odio, ocupación ilegal de vivienda, maltrato animal.
- Zonas “Guardián público”, dónde el ciudadano puede compartir su posición con los servicios de rescate, para los peregrinos del Camino de Santiago, por ejemplo.
- Botón S.O.S. para los colectivos de violencia de género (Viogen) y sanitario con las FFCCSE y botón S.O.S. entre particulares.
- Sistemas para la localización de desaparecidos en zonas sin cobertura través de la señal wifi del smartphone.
- Integración de los centros de recepción de alarmas de las empresas de seguridad privada.
- AML, servicio para la localización de las llamadas de emergencias al 091 y 062.

Desde AlertCops se da servicio a más de 1.200.000 usuarios registrados, en 6.993 municipios, y se han atendido más 130.000 situaciones de riesgo, desde 100 centros de atención de la Policía Nacional y de la Guardia Civil. Los medios de comunicación se han hecho eco de multitud de casos de éxito.

Figura 6. Sistema AlertCops. Fuente: elaboración propia.

AlertCops, como servicio eficaz e innovador, ha recibido múltiples reconocimientos internacionales y nacionales.

Actualmente se está trabajando en una versión totalmente renovada de AlertCops. Fruto del análisis y de las opiniones de los usuarios y las FFCCSE, se identificaron las funcionalidades más valiosas (como el servicio Acompáñame) y las líneas de diseño y criterios de usabilidad más convenientes. El objetivo es que AlertCops se perciba como una aplicación sencilla y fácil de usar y con capacidades muy valiosas para los ciudadanos y las FFCCSE, no solamente para solicitar atención policial sino también para obtener información. Gracias al resultado de este análisis, se ha realizado un rediseño integral de toda la plataforma que se desplegará en AlertCops v7 durante el año 2023.

3.- ESTRATEGIA

El reconocimiento de estos proyectos tanto a nivel nacional como internacional (UE) obliga a continuar con el esfuerzo en materia tecnológica y, para ello, la SGSICS ha diseñado un Plan Estratégico que recoge las actuaciones a desarrollar dentro de los próximos cinco años, continuando así con los objetivos de modernización tecnológica de nuestras FFCCSE. En dicho plan, destacan las siguientes líneas de acción:

- La permanente actualización de todos aquellos proyectos en servicio y el desarrollo de los nuevos proyectos necesarios para mantener los estándares de seguridad requeridos a nivel internacional.
- La consolidación del Centro Tecnológico de Seguridad, como herramienta tecnológica de apoyo a las operaciones e intercambio de información entre las FFCCS, incluyendo las siguientes iniciativas:
- Establecimiento del Nuevo Centro de Proceso de Datos (CPD) para la Seguridad en las instalaciones del CETSE en El Pardo, diseñado desde la perspectiva de la eficiencia en el marco del ahorro energético y el respeto al medio ambiente, así como con una arquitectura de sistemas, almacenamiento y comunicaciones que sea

compatible con la infraestructura actualmente existente en los CPD de la SGSICS, Policía Nacional y Guardia Civil que permita un funcionamiento en modo activo-activo como Centro de Respaldo de los anteriores.

- Desarrollo de un Centro de Supercomputación para la Seguridad que proporcione capacidad para la implantación de nuevos desarrollos de alto nivel para las FFCCSE, de una manera armonizada, redundando en una mejora clara de la eficiencia, tanto técnica como económica, de las inversiones presentes y futuras.
- Diseño de un Centro de Monitorización de Sistemas (Fusion Center), que permitirá mejorar la fusión de información entre sistemas y el intercambio de datos entre diversas fuentes (incluyendo FFCCSE, sector público y privado) y el control de la actividad de los sistemas tecnológicos a través de la monitorización de sus indicadores.

4.- EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN NUESTRO ENTORNO

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) define la Inteligencia Artificial (IA) como: "un sistema que puede, para un conjunto de objetivos específicos, realizar predicciones, recomendaciones o decisiones que influyan en entornos reales o virtuales".

En nuestro caso, la definición de IA debe ser tan neutra como sea posible, con el objeto de abarcar todas las tecnologías que el término comprende y aquellas que están aún por desarrollar. El objetivo es abarcar toda la IA, incluyendo desde el aprendizaje de máquina (Machine Learning) hasta los sistemas híbridos y de aprendizaje profundo (Deep Learning).

En el marco europeo, la Dirección General de Migración y Asuntos de Interior (DG HOME) de la Comisión Europea también está debatiendo en la actualidad, junto con la Dirección General de Redes de Comunicación, Contenido y Tecnologías (DG CONNECT), EUROPOL, la Agencia eu-LISA y los Estados Miembros (EEMM), las diferentes opciones de arquitectura para espacios seguros de datos y los requisitos técnicos en base a los principios legales vigentes para la implantación de la IA. Prueba de ello, fue la creación en el año 2019 del Grupo de Trabajo IA de Eu-Lisa (WGAI Working Group Artificial Intelligence), en el que el Ministerio del Interior participa a través de la SGSICS.

En 2018 la Comisión Europea creó el Grupo de Expertos de Alto Nivel sobre Inteligencia Artificial (IA HLEG)[1], dedicado a elaborar las estrategias y hacer las correspondientes recomendaciones en materia IA. En 2019, la Comisión Europea publicó unas directrices sobre una IA fiable y una lista de evaluación para 2020, basándose en los valores comunes de todos los Estados Miembros en el Espacio de Libertad, Seguridad y Justicia (ELSJ). No se pretendía cambiar la legislación existente, eran recomendaciones no vinculantes, que, previa consulta de los distintos interesados (stakeholders), marcarán los requisitos claves para una IA confiable socialmente en ámbitos como el de la seguridad, la protección de datos de carácter personal, la privacidad o las reglas de protección medioambiental.

[1] El representante de España, pertenece al Ministerio del Interior.

Con el propósito fomentar un marco de confianza de la ciudadanía en la IA, basado en el respeto de los principios éticos, legales y morales del espacio europeo, y de examinar la viabilidad y los elementos, sobre la base de consultas con las múltiples partes interesadas, de un marco jurídico para el desarrollo, el diseño y la aplicación de la inteligencia artificial, basado en las normas del Consejo de Europa sobre derechos humanos, democracia y Estado de Derecho, el 11 de septiembre de 2019, el Comité de Ministros del Consejo de Europa creó el Comité Ad Hoc sobre Inteligencia Artificial (CAHAI). El CAHAI tiene una composición única ya que reúne a los EEMM y observadores, así como integrantes de la sociedad civil, el mundo académico y el sector privado.

Trabaja en estrecha colaboración con otras instituciones internacionales, como la UNESCO (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura), la OCDE y la Unión Europea. La SGSICS en representación del Ministerio del Interior junto con el Ministerio de Justicia y el Ministerio de Asuntos Exteriores, son los miembros españoles en dicho Comité.

El CAI (evolución del CAHAI), es el Comité sobre IA del Consejo de Europa para el período 2022-2024, encargado de establecer un proceso de negociación internacional que permita elaborar un marco jurídico para el desarrollo, la concepción y la aplicación de la IA a nivel internacional.

En términos estratégicos, la SGSICS se ha alineado con la Estrategia de la UE para la Unión en Seguridad y con las líneas estratégicas marcadas por Comisión Europea para la Década Digital y, por tanto, contribuir a cumplir los objetivos digitales para 2030 desde el punto de vista de la seguridad. Este marco debe garantizar que la tecnología de IA pueda desarrollarse e implementarse en Europa y en España y al mismo tiempo garantice que la referida tecnología no se utilice de manera inapropiada.

Para poder hacer frente a estas problemáticas, la SGSICS ha definido una estrategia interna de IA aplicada a las nuevas tecnologías para implantar en el Ministerio del Interior, alineada tanto con la Estrategia Nacional de Inteligencia Artificial (ENIA), como con la Estrategia Española de I+D+i en IA del Ministerio de Ciencia, Innovación y Universidades. En torno a este objetivo se configuran los siguientes Ejes Estratégicos para el ámbito de la Seguridad y la IA:

- Posicionar a las FFCCSE, y resto de organismos dependientes de la Secretaría de Estado de Seguridad, como elemento primordial en el desarrollo de IA, utilizando el potencial tecnológico como catalizador de su conocimiento y experiencia.
- Promover la evaluación de la adecuación tecnológica del nuevo sistema con las necesidades funcionales y operativas en condiciones de utilización reales.
- Fomentar un marco de confianza en las tecnologías derivadas de la IA, mediante la utilización legal, ética y segura, la protección de las libertades civiles, la privacidad y los valores de los ciudadanos, aprovechando plenamente el potencial que las nuevas tecnologías ofrecen en materia de seguridad.
- Estrategia común de datos e interoperabilidad, adaptada a los estándares europeos y a los proyectos europeos de gran magnitud coordinados tanto por la Comisión Europea como por las Agencias Europeas, eu-LISA y Europol.
- Búsqueda y fomento del talento, formación y desarrollo de competencias y habilidades en materia de IA dentro del Ministerio del Interior.

- Impulsar los avances tecnológicos en IA a través de la colaboración y trabajo conjunto público-privado establecido por el Gobierno, con el fin de promover la competitividad y la Seguridad Nacional.
- Promover y participar activamente en foros nacionales e internacionales, apoyando la investigación, el desarrollo, la innovación, la implementación y la adquisición en materia de IA.

5.- INVESTIGACIÓN, DESARROLLO E INNOVACIÓN

Con respecto a la actividad de Investigación, desarrollo e innovación (I+D+i), conforme al Real Decreto 734/2020 de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior y el Real Decreto 146/2021, de 9 de marzo, por el que se modifican el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales, y el Real Decreto 734/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior, la SGSICS es la encargada de "Acordar, coordinar, ejecutar y llevar a cabo cualquier otra acción necesaria relativa a la participación en proyectos europeos de investigación, desarrollo e innovación (I+D+i) en materia de seguridad" de acuerdo con las instrucciones del Secretario de Estado, así como de "Dirigir el Centro Tecnológico de Seguridad (CETSE) como órgano de implementación de las funciones específicas de esta Subdirección y de las políticas de I+D+i del órgano Directivo".

Específicamente, el Departamento de I+D+i del CETSE tiene, entre sus funciones, la coordinación de la participación del Ministerio de Interior en proyectos de Innovación. Desde este departamento se gestionan actualmente más de 80 proyectos internacionales de distintos programas de financiación europea, entre los que se encuentran Horizonte Europa, Fondos de Seguridad Interior (Internal Security Fund, FSI), Programa Ciudadanos, Igualdad, Derechos y Valores (Citizens, Equality, Rights and Values Programme, CERV), Fondo de Defensa Europeo (European Defence Fund, EDF) o Compra Pública Innovadora, entre otros, dando apoyo en la gestión de los mismos a todos los organismos dependientes del Ministerio del Interior como son: Policía Nacional, Guardia Civil, Instituciones Penitenciarias, Protección Civil, la Oficina Nacional de Lucha Contra los Delitos de Odio (ONDOD), la Dirección General de Apoyo a las Victimas del Terrorismo, OCC, CNPIC o el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO).

Igualmente se trabaja en el desarrollo de proyectos de I+D+i nacionales, según las necesidades de los usuarios finales del Ministerio del Interior.

Así mismo, se participa activamente en diferentes redes y grupos de trabajo internacionales, siendo puntos nacionales de contacto. Algunos ejemplos son: ENLETS (Red Europea de Servicios de Tecnología para la aplicación de la Ley), IFAFRI (Foro internacional para promover la innovación en primeros auxilios), I-LEAD (Innovation - Law Enforcement Agencies Dialogue) y AHEAD (TowArd sustainable foresigHt capabilitiEs for increAseD Civil Security).

Otra de las actividades de gran peso del departamento es la dirección y gestión de la comunidad de usuarios (COU Spain). Esta iniciativa pone en contacto a la academia, la industria y los usuarios finales –FFCCSE, Policías Autonómicas, Policías Locales, Cuerpos de Emergencias, etc., tanto a nivel nacional como regional y local–, con el

objetivo de llevar a cabo proyectos de interés para todos. La COU está en contacto y colaboración constante con la Comunidad de Usuarios Europea (CERIS), así como con otras redes internacionales en el ámbito de la seguridad con las que se mantiene una estrecha colaboración.

Actualmente se está trabajando en el desarrollo y la implementación del Nodo Nacional de EACTDA (European Anti-Cybercrime Technology Development Association) a través de la COU, con el objetivo de facilitar las herramientas desarrolladas en los proyectos europeos a los usuarios finales españoles.

6.- TRANSFORMACIÓN DIGITAL

En aras de dar cumplimiento a las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y alineados con los principios rectores del Plan de Transformación Digital 2015-2020 de la Administración General del Estado y sus Organismos Públicos, la SGSICS está implantando en el Ministerio del Interior una nueva arquitectura basada en tecnología de microservicios, que posibilitará ofrecer servicios de alta disponibilidad con capacidades de adaptación al cambio, necesarios para la tramitación electrónica de procedimientos administrativos.

Parte central de esta plataforma será la Plataforma de Servicios de Administración Digital (SAD) cuyo objetivo principal será asegurar y simplificar la integración de todas las aplicaciones y sistemas de tramitación del Ministerio del Interior con los principales servicios de Administración Digital. Esta plataforma permitirá dar uniformidad a los proyectos del Ministerio, garantizando el uso de expedientes electrónicos, sistemas de firma electrónica y comunicación prioritaria electrónica con los ciudadanos. Asimismo, parte de dicha arquitectura será la Plataforma de Integración con Terceros, que concentrará en un nodo de comunicación, la interacción electrónica con otras Administraciones y organismos nacionales e internacionales en el ámbito civil.

Por otra parte, y con el objetivo de atender las demandas en materia de Protección Internacional de la Oficina de Asilo y Refugio (OAR), se requiere disponer de una aplicación de alta seguridad que gestione el ciclo de vida completo de los expedientes de solicitud de protección internacional, apátridas y refugiados. Actualmente, la OAR, utiliza la aplicación Asilo, desarrollada en 2006. Las necesidades y la tecnología existente en 2006 distan mucho de las existentes en la actualidad. La aplicación se desarrolló para un número de usuarios muy limitado, teniendo en cuenta el fuerte incremento que se ha dado en los últimos tiempos.

Durante 2022 se ha continuado con el desarrollo de la nueva aplicación para el Sistema Integral de Gestión de Solicitudes de Protección Internacional, llamado LARES. En un entorno de crecimiento exponencial de las solicitudes, este año se ha superado el número de solicitudes, llegando a 118.842. Esta nueva aplicación incluye mejoras que permiten una mayor capacidad de tramitación. Las mejoras se implementan a varios niveles:

- La gestión diaria de las solicitudes y resoluciones de Protección Internacional se rediseña, creando una nueva forma de trabajo automatizada y adaptable al contexto de cada país.

- A nivel técnico, se están configurando algunos aspectos técnicos clave como el empleo de una arquitectura orientada a microservicios, lo que supone un cambio de paradigma en la forma de afrontar nuevos desarrollos de cara al futuro.
- Desde el punto de vista de la usabilidad, se ha creado una nueva interfaz, que ofrece un entorno más fácil de manejar para los usuarios de la aplicación. La nueva interfaz se diseña como punto principal de entrada de datos, lo que ayudará en el flujo de información entre las diferentes fuentes, tanto de Policía como de la SG de Protección Internacional.
- Adicionalmente, se ha innovado en la metodología de trabajo. Se ha utilizado una metodología "User eXperience Design" para la confección junto con los usuarios de tableros con post-it en los que se recoge toda la funcionalidad definida.
- A nivel estratégico, se sigue evolucionando en el sistema para que permite la elaboración de informes dinámicos e interactivos con información actualizada a diario. Dichos informes son personalizables y accesibles, tanto para las unidades gestoras, como para los altos cargos responsables de dichas unidades.

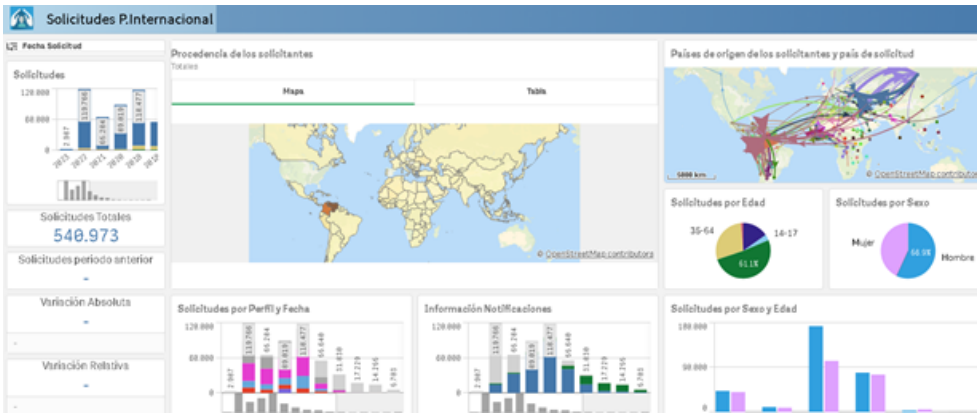

Figura 7. Cuadro de mando de LARES. Fuente: elaboración propia.

En este ámbito, destaca la implementación del proceso de resoluciones de protección temporal en un máximo de 24 horas, de acuerdo a la Orden PCM/169/2022, de 9 de marzo, por la que se desarrolla el procedimiento para el reconocimiento de la protección temporal a personas afectadas por el conflicto en Ucrania.

Dicho procedimiento ha permitido tramitar más de 150.000 solicitudes de protección temporal desde su comienzo, el 11 de marzo de 2022. Asimismo, se ha preparado un mecanismo rápido y sencillo que permite a los ciudadanos ucranianos descargarse su resolución de protección temporal directamente de la página web del Ministerio del Interior.

Otro ejemplo del aprovechamiento de sinergias entre los integrantes del CETSE es la capacidad para velar por la seguridad y el buen funcionamiento de los procesos de escrutinio electoral, en los cuales España se sitúa como referencia a nivel mundial. El trabajo conjunto de funcionarios y Fuerzas y Cuerpos de Seguridad del Estado está permitiendo reducir paulatinamente la dependencia tecnológica en este ámbito, lo cual repercutirá en un considerable ahorro de coste y mejora de calidad a medio plazo. En este proceso se realizan múltiples tareas para garantizar el correcto funcionamiento de los sistemas informáticos que realizan el escrutinio durante la noche electoral.

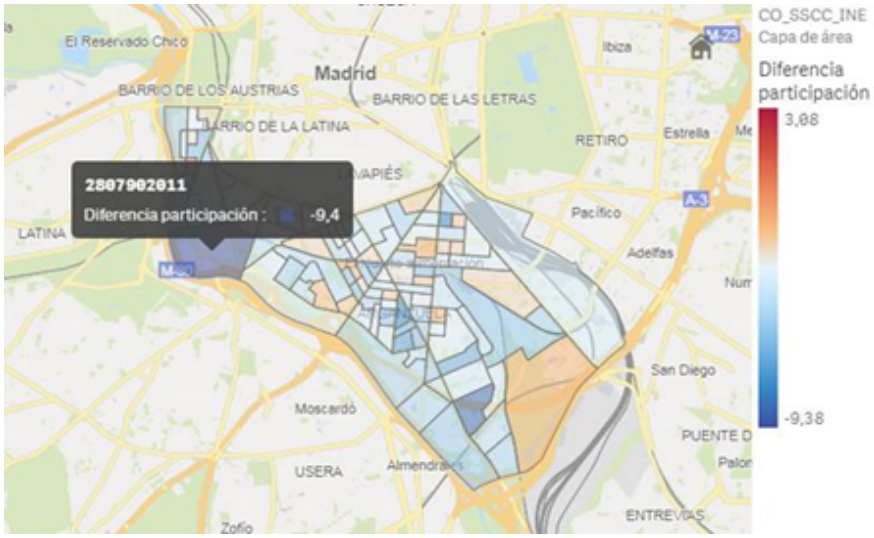

Figura 8. Detalle de la herramienta de visualización de resultados electorales.
Fuente: elaboración propia.

Se auditan los sistemas informáticos, los servidores y las comunicaciones a todos los niveles, se supervisan las pruebas realizadas por el adjudicatario y se realizan pruebas complementarias que garanticen el correcto funcionamiento del escrutinio electoral, desde la recogida de candidaturas de partidos políticos hasta la publicación en BOE del escrutinio definitivo, pasando por la difusión provisional de resultados de la jornada electoral.

Así mismo, se han iniciado nuevas líneas de trabajo, como la puesta en marcha de un sistema de visualización de resultados electorales que permite, a las pocas horas de celebración de las elecciones generales, realizar análisis evolutivos del detalle del voto o de la participación, llegando al nivel de mesa electoral.

7.- CONCLUSIONES

En definitiva, el conjunto de las actuaciones descritas, así como los numerosos desarrollos transversales de apoyo a las mismas, llevados a cabo en el ámbito del Centro Tecnológico para la Seguridad de la Secretaría de Estado de Seguridad, nos permiten ir adaptando el funcionamiento del Ministerio a la realidad digital del entorno social, a través de la provisión de servicios de valor cada vez más eficaces y eficientes, de una manera rápida y segura, garantizando, en todo momento, los derechos fundamentales de los ciudadanos en un espacio de libertad, seguridad y justicia.

Glosario

ABC	Automated Border Control, Control Automatizado de Fronteras.
ABIS	Automatic Biometric Identification System, Sistema Automático de Identificación Biométrica.
AENA	Aeropuertos Españoles y Navegación Aérea.
AML	Advanced Mobile Location, Localización Móvil Avanzada.
CAHAI	Ad hoc Committee on Artificial Intelligence, Comité Ad Hoc sobre Inteligencia Artificial.
CERIS	Community for European Research and Innovation, Comunidad para la Investigación y la Innovación Europeas.
CERV	Citizens, Equality, Rights and Values Programme, Programa Ciudadanos, Igualdad, Derechos y Valores
CETSE	Centro Tecnológico de Seguridad.
CITCO	Centro de Inteligencia contra el Terrorismo y el Crimen Organizado.
CIR	Common Identity Repository, Repositorio Común de Identidades.
CNPIC	Centro Nacional para la Protección de Infraestructuras Críticas.
COU	Community of Users, Comunidad de Usuarios.
CPD	Centro de Proceso de Datos.
EACTDA	European Anti-Cybercrime Technology Development Association, Asociación europea de desarrollo de tecnología contra el ciberdelito.
ECRIS-TCN	European Criminal Records Information System - Third Country Nationals, Sistema Europeo de Información de Antecedentes Penales: información sobre condenas de nacionales de terceros países.
EEMM	Estados Miembros.
EES	Entry Exit System, Sistema de Entradas y Salidas.
ELSJ	Espacio de Libertad, Seguridad y Justicia.
ENIA	Estrategia Nacional de Inteligencia Artificial.
ENLETS	European Network of Law Enforcement Technology Services, Red Europea de Servicios de Tecnología para la aplicación de la Ley.
ESP	European Search Portal, Portal Europeo de Búsqueda.
ETIAS	European Travel Information and Authorization System, Sistema Europeo de Información y Autorización de Viajes.
eu-LISA	Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia.
Eurodac	Sistema europeo de comparación de impresiones dactilares de los solicitantes de asilo.
FFCCSE	Fuerzas y Cuerpos de Seguridad del Estado.
FSI	Fondos de Seguridad Interior
HLEG	High-Level Expert Group, Grupo de Expertos de Alto Nivel.
I+D+i	Investigación, Desarrollo e Innovación.
IA	Inteligencia Artificial.
IFAFRI	International Forum to Advance First Responder Innovation, Foro internacional para promover la innovación en primeros auxilios.
MID	Multiple-Identity Detector, Detector de Identidades Múltiples.
OAR	Oficina de Asilo y Refugio.
OCC	Oficina de Coordinación Cibernética.
OCDE	Organización para la Cooperación y el Desarrollo Económicos.
ONDOD	Oficina Nacional de Lucha Contra los Delitos de Odio.
PNR	Passenger Name Record, Sistema de Registro de Nombres de Pasajeros.

SAD	Servicios de Administración Digital.
SAID	Sistema Automático de Identificación Dactilar.
SBMS	Shared Biometric Matching Service, sistema de correspondencia biométrica compartida.
SGSICS	Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad.
SIGLO-CD	Sistema Global Contra Drones.
SIRDEE	Sistema de Radiocomunicaciones Digitales de Emergencia del Estado.
SIS	Schengen Information System, Sistema de Información Schengen.
TCN	Third Country Nationals, Ciudadanos de Terceros Países.
UE	Unión Europea.
UNESCO	United Nations Educational, Scientific and Cultural Organization, Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.
VIS	Visa Information System, Sistema de Información de Visados.
WGAI	Working Group Artificial Intelligence, Grupo de Trabajo sobre Inteligencia Artificial.