

NEWS ADSI FLASH



www.adsi.pro

Salón Internacional de la Seguridad 2018

Índice

- *Nuestros Patrocinadores..* 2
- *Salón Internacional de la Seguridad (SICUR) 2018 .* 3
- *Los ultras no se han ido del fútbol español.....* 7
- *Los datos de los pasajeros ya pueden cruzarse con las bases policiales.....* 9
- *EURO DEFENSE ESPAÑA.....* 11
- *Análisis sobre dispositivo de seguridad para la copa mundial de futbol 2018 en Rusia* 13
- *El foro Davos lanza un Centro Global para la Ciberseguridad a partir de marzo* 16
- *Cuarteles militares secretos hechos públicos por las pulseras deportivas.....* 17
- *Los estrategias policiales proactivas ¿son útiles?...* 19
- *Protección de datos, ¿qué novedades se avecinan?* 20
- *Noticias.....* 21
- *Formación* 22
- *Legislación* 23
- *Revistas.....* 23

The poster features the SICUR logo at the top, which consists of a stylized arch with blue and orange segments. Below the logo, the text reads: "SICUR", "Salón Internacional de la Seguridad", and "International Security, Safety and Fire Exhibition". The dates "20-23 FEB. 2018" are prominently displayed in orange. At the bottom, it states "ORGANIZA ORGANISED BY IFEMA Feria de Madrid" with the IFEMA logo. The website "www.sicur.ifema.es" and contact information "IFEMA - Feria de Madrid Tel. 902 22 15 15 · (34) 91 722 30 00 · sicur@ifema.es" are provided at the very bottom.

Nuestros Patrocinadores



ASTRA

Su seguridad, al día



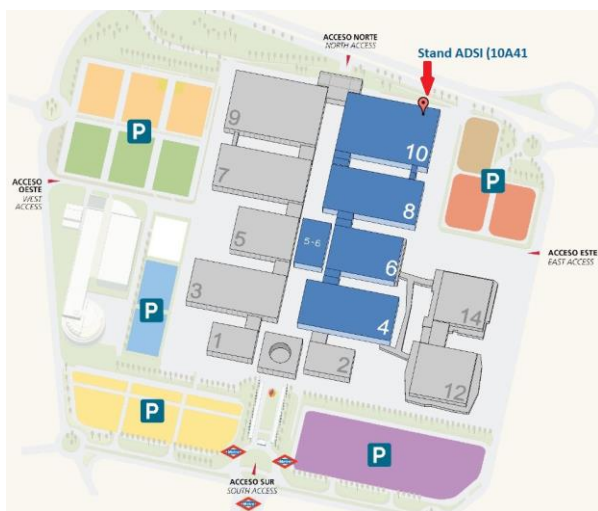
DATABAC
Soluciones completas de identificación



Salón Internacional de la Seguridad (SICUR) 2018

Como cada año, **ADSI** dispondrá de stand en el Salón Internacional de la Seguridad 2018 (SICUR).

El stand con numeración **10A41** se encuentra situado en la siguiente ubicación:



Crecer en representatividad, en convocatoria profesional, nacional e internacional, y elevar la relevancia y visibilidad que ya tiene SICUR, como punto de encuentro sectorial, objetivos de esta edición.

Organizada por IFEMA, SICUR 2018 se celebrará del 20 al 23 de febrero de 2018 en Feria de Madrid.

SICUR, Salón Internacional de la Seguridad, ha comenzado los preparativos para la celebración de su próxima convocatoria que, organizada por **IFEMA**, tendrá lugar en los pabellones de la **Feria de Madrid, del 20 al 23 de febrero de 2018**.

Uno de los primeros pasos ha sido reunir a su recién constituido Comité Organizador, el pasado 13 de junio, con el objetivo de presentar los ejes que caracterizarán esta nueva edición y trabajar en la estrategia orientada a crecer en la representatividad del mercado, en convocatoria profesional, nacional e internacional, así como en elevar la relevancia y visibilidad que ya tiene **SICUR**, como punto de encuentro sectorial.

Y todo apunta a que **SICUR 2018** será una gran feria, y que superará los parámetros conseguidos en la edición de 2016, en la que registró crecimientos del 11% en participación - 1.332 empresas; del 24% en superficie, con la ocupación de 27.984 m², y del 8,5% en visitas, con la asistencia de 42.294 profesionales de 76 países.

A estos datos, que abren expectativas muy positivas, se suma, una vez más el fuerte respaldo de las principales Asociaciones que representan al mundo de la seguridad en

ADSI en el Salón Internacional de la Seguridad 2018

todas sus vertientes, entre las que se encuentran **TECNIFUEGO/AESPI**, Asociación Española de Sociedades de Protección Contra Incendios, al frente de la presidencia del Comité Organizador; **ASEPAL**, Asociación de Empresas de Equipos de Protección Laboral; **AES**, Asociación Española de Empresas de Seguridad, y **APROSER**, Asociación de Compañías Privadas de Servicios de seguridad, en las tres vicepresidencias. También forman parte de este Comité las principales asociaciones representativas del mundo de la seguridad privada, seguridad laboral, el mundo de la prevención, profesionales, cuerpos y fuerzas de seguridad pública, configurando un completo grupo de trabajo enfocado a fomentar una mayor involucración del tejido industrial al que da servicio **SICUR** y mejorar la interacción entre expositores y organización para un eficaz desarrollo de la feria y de sus actividades.

La oferta de **SICUR** se presentará lo largo de cuatro pabellones, en los que cada uno de los sectores cuenta con su propia identidad. El pabellón 10, dedicado a **Security**, concentrará lo último en equipos para la seguridad física, el control de intrusión y de accesos, la vigilancia, soluciones en seguridad privada, los equipamientos para las fuerzas públicas de seguridad, y en general los últimos avances tecnológicos al servicio de la protección de bienes. En el pabellón 8, donde se sitúa el Sector **Contra Incendios y Emergencias** se mostrarán las novedades en seguridad pasiva y activa contra el fuego, así como en las soluciones para mejorar la respuesta en situaciones de emergencia, **y en los pabellones 4 y 6 se encontrará el sector de Seguridad Laboral, que presentará las propuestas en nuevos Elementos de Protección Individual (EPI)**, así así como en medidas de prevención y salud laboral.

Como es habitual, **SICUR** también se convertirá en un importante escenario divulgativo y análisis de la actualidad sectorial, a través de las distintas ponencias y presentaciones que ofrecerá **Foro SICUR**, en un formato orientado al debate, a lo que se sumaran múltiples **exhibiciones, demostraciones y pruebas de producto** de gran dinamismo, y una nueva convocatoria de la **Galería de Nuevos Productos** que ofrecerá una interesante panorámica de la labor de investigación y desarrollo sectoriales.



20-23

Feb.

2018

[Actividades](#)[Registro](#)[Información](#)

Seguridad contra incendios y emergencias

Instalaciones, equipos, vehículos de bomberos, sistemas de detección y extinción... Toda una oferta especializada en protección activa y pasiva contra el fuego y soluciones para mejorar la respuesta en situaciones de emergencia



Fire safety and emergency

Plant, equipment, fire fighting vehicles, fire detection and extinction systems... a whole range of specialised products for the active and passive protection against fire and solutions to improve the response in emergency situations



Seguridad Laboral

Los Equipos de Protección Individual -EPI's-, la prevención de riesgos y la salud laboral tienen su mejor referente en este espacio protagonizado por el diseño, la tecnología y los nuevos materiales, al servicio del confort y la protección

Safety and health at work

Individual Protection Equipment -IPE-, risk prevention and occupational health are of utmost importance in this category where design, technology and new equipment play key roles in offering comfort and protection

EL GRAN REFERENTE INTERNACIONAL EN ESPAÑA DE LA SEGURIDAD

Punto de encuentro para empresas, asociaciones, profesionales y usuarios de la seguridad

SICUR, Salón Internacional de la Seguridad, reúne cada dos años en Madrid a proveedores de equipos y soluciones de seguridad con toda la cadena de valor del sector y con la representación profesional de los usuarios de seguridad en los sectores público y privado.

La innovación y el desarrollo tecnológico protagonizan este encuentro profesional que aborda la seguridad integral y se desarrolla en distintas áreas; Seguridad Contra Incendios y Emergencias, Seguridad Laboral, Security, que engloba Seguridad Privada y Pública y Defensa.

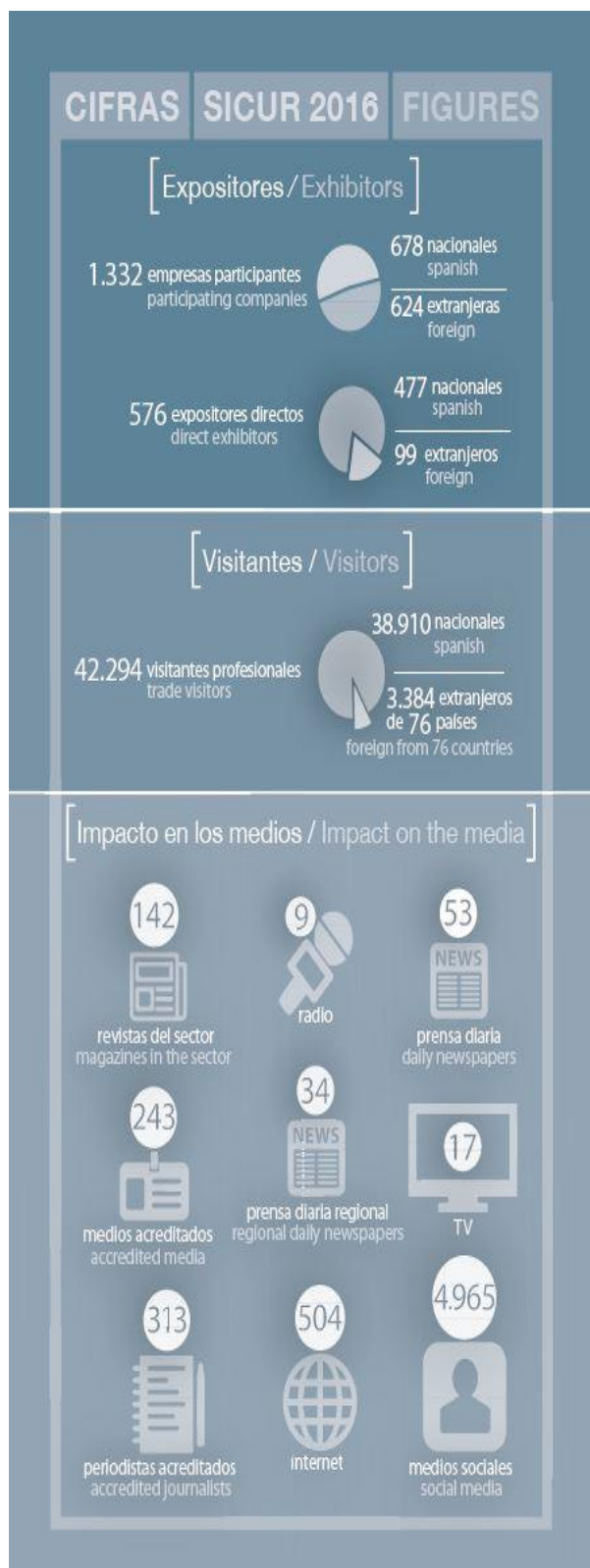


THE GREAT INTERNATIONAL REFERENCE IN SPAIN OF SAFETY AND SECURITY

The meeting point for companies, associations, professionals and users of safety and security

SICUR, International Security, Safety and Fire Exhibition, is held every two years in Madrid and brings together suppliers of equipment and safety and security solutions, players from the entire value chain in the sector and professional representatives of safety and security users from the public and private sectors.

Innovation and technological development are the main features of this professional event which covers end-to-end security organised under different categories: Fire and Emergency Safety; Occupational Safety; Security, which encompasses Private and Public Security, in constant interaction and Defence.



¿POR QUÉ PARTICIPAR EN SICUR 2018? WHY CHOOSE SICUR 2018?

NEGOCIO

BUSINESS

Identificar nuevos clientes, consolidar relaciones comerciales y explicar nuevas oportunidades de negocio.

Identify new customers, consolidate business relationships and explain new business opportunities.

RED DE CONTACTOS NETWORK OF CONTACTS

Punto de encuentro donde podrá gestionar sus reuniones con la base de datos de visitantes profesionales.

Meeting point to manage your meetings with the trade visitor database.

INNOVACIÓN

INNOVATION

SICUR es el lugar elegido por numerosas empresas para presentar sus novedades.

SICUR is the industry's event of choice for presenting innovations for many companies.

CONOCIMIENTO

KNOWLEDGE

Amplio programa de Jornadas técnicas, mesas redondas, presentaciones y actividades paralelas, caracterizadas por la gran diversidad de temas, así como por el alto nivel de los participantes y ponentes.

A comprehensive program of technical workshops and parallel activities, on a wide range of subnets, with a high level of participants and speakers.

ACTIVIDADES / ACTIVITIES



Amplio programa de jornadas técnicas, conferencias y debates donde se abordan temas transversales de interés para los usuarios de la seguridad de todos los sectores de la actividad, con un formato muy dinámico y orientado al debate.

Extensive programme of technical workshops, conferences and discussions.



Espacio dedicado a reconocer el esfuerzo en I+D+I de las empresas expositoras.

New Products Gallery

Features the latest products from exhibiting companies, showcase the latest innovations.

EXHIBICIONES



Programa de actividades dinámicas con demostraciones en directo de diversas actuaciones en situaciones de riesgo y emergencias, pista de demostraciones de RPAS en vuelo, exposición de vehículos antiguos de policía...

Dynamic programme of activities

With live demonstrations of response actions for risk and emergency situations.



Security

Sistemas inteligentes de control de acceso y de alarmas. Video vigilancia, lectores biométricos, geolocalización, drones, cerraduras, barreras y cajas de seguridad, servicios para la gestión de la seguridad, equipamiento para fuerzas y cuerpos de seguridad... la innovación tecnológica al servicio de la protección de bienes y vidas



Security

Smart systems for controlled access and alarms. Video-surveillance, biometric readers, geolocation, drones, locks, barriers and safes, security management systems, equipment for law enforcement authorities... technological innovation serving to protect property and lives

Defence

The defence industry converges with the civil market in this space. Naval, aeronautical and space equipment, land vehicles, border protection... advanced safety and security solutions which, developed in the world of defence, are then transferred to the entire safety and security market

Defensa

La industria de la defensa converge con el mercado civil en este espacio. Equipamiento naval, aeronáutico y espacial, vehículos terrestres, protección de fronteras... soluciones avanzadas de seguridad que, desarrolladas en el ámbito de la defensa, se transfieren a todo el mercado de la seguridad

Los ultras no se han ido del fútbol español

Fuente: El Mundo
Eduardo J. Castela

EL MUNDO

Pese a que sólo nueve grupos aparecen en el listado de Antiviolenencia, son muchos los que siguen protagonizando incidentes cada semana.

"La Comisión no hace cumplir la ley y se pone de perfil. El Observatorio contra la violencia en el deporte no se reúne desde hace muchos años", explica Esteban Ibarra, presidente del Movimiento contra la Intolerancia

Conversación de Whatsapp. Jueves 18 de enero.

- *Hola, ¿cómo estás? ¿qué pasó ayer? ¿hubo lío otra vez?*
- *Sí, pero es injusto que se relacione al Frente con eso. El que apuñaló no pertenece al Frente.*
- *Bueno, pero cuéntame algo más.*
- *Por aquí no, no me fío mucho de los móviles.*

En el Frente Atlético, en sus alrededores, el jueves 18 de enero era un día difícil. Corrían, con muchísima cautela, los mensajes, las versiones, las fotos y hasta los vídeos de lo que había pasado media hora antes del Atlético-Sevilla del pasado miércoles en las proximidades del Wanda. La versión del club rojiblanco coincidía: «**No eran del Frente**». Un Frente Atlético, por cierto, expulsado como peña del club tras la muerte de *Jimmy*, el ultra del Deportivo de la Coruña (2014).

Este pasado mes de enero, dos acontecimientos han devuelto el foco hacia los ultras del fútbol. El apuñalamiento en las cercanías del Wanda y la invasión, el pasado martes 16 de enero, de un grupo de Biris -los radicales del Sevilla- del entrenamiento del equipo, logrando incluso conversar con una representación de la plantilla. La pregunta es obvia: ¿se han marchado los violentos de los campos? La respuesta es sencilla: no. Tras la brusca concienciación colectiva que supuso el asesinato de *Jimmy*, con el Real Madrid emulando al Barça en la extirpación de sus grupos, se había instalado en el ambiente algo parecido al olvido del problema. Y el problema sigue aquí.

Quizá no en los documentos oficiales, pero sí en la realidad de los telediarios. Un informe de la Comisión Estatal contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte (para resumir, la Comisión Antiviolenencia) remitido el pasado 6 de octubre a la Federación Española identifica como «grupos radicales y/o violentos» apenas a nueve. Son

estos: **Frente Atlético (Atlético de Madrid)**, **Riazor Blues (Deportivo)**, **Biris-Biris Norte (Sevilla)**, **Frente Bokerón y Malaka Hinchas (Málaga)**, **Irautza (Alavés)**, **Ligallo Fondo Norte y Avispero (Zaragoza)** y **Jove Elx (Elche)**. De ellos, seis están hoy en Primera División. Eso son los papeles oficiales. Esto, las páginas de los periódicos: 10 de septiembre de 2017: «Los ultras del Sporting, a palos con la Policía». 9 de octubre de 2017: «Varios ultras revientan la manifestación del Día de la Comunidad Valenciana. El juez identifica a 13 agresores, nueve de ellos pertenecen a los Yomus, el grupo de ultras seguidores del Valencia Club de Fútbol». 5 de enero de 2018: «Veinticuatro aficionados radicales del Sevilla y del Betis fueron detenidos por la Policía tras una pelea». 17 de enero de 2018: «El Espanyol prohíbe la entrada a 150 Boixos Nois que iban con bengalas y palos».

Un parámetro curioso

Ni los Boixos Nois (Barcelona), ni los Yomus (Valencia), ni los Supporters Gol Sur (Betis), ni los Ultra Boys (Sporting) ni las Brigadas Amarillas (Cádiz) aparecen en la lista de Antiviolenencia y, sin embargo, han protagonizado peleas de extrema gravedad en los últimos meses. ¿Por qué? Antiviolenencia, en el informe remitido a la Federación -que esta a su vez envió a los clubes- establece un parámetro para elaborar la lista de grupos violentos. Deben ser «grupos de seguidores que hayan incurrido en las conductas definidas en los apartados primero y segundo del Artículo 2 de la Ley 19/2007 contra la violencia, el racismo, la xenofobia y la intolerancia en el deporte».

Grupos radicales en los clubes de fútbol

Señalados como grupos ultras por la Comisión Nacional Antiviolenencia



(1): Sustituidos por la Grada de animación.

(2): Había un grupo llamado Colectivo Aldeano, pero ya se disolvieron.

FUENTE: Elaboración propia.

EL MUNDO GRÁFICOS

En esos apartados se habla, entre otras cosas, de «participación activa en altercados, riñas, peleas o

desórdenes públicos en los recintos deportivos, en sus alrededores o en los medios de transporte organizados para acudir a los mismos». Incumplen muchas más conductas, pero sólo ese apartado sirve para ver cómo la lista es excesivamente corta. «El resto de grupos ultras no aparecen en ese listado porque han sido erradicados de los estadios. Por ejemplo, los Yomus como tal no existen, el Valencia tiene una grada fan con todos sus miembros identificados», sostiene una fuente autorizada, conocedora de estos asuntos. Sin embargo, y en teoría, el Frente Atlético tampoco existe como peña oficial del Atlético y, sin embargo, sí está en ese listado. Y también sin embargo, y también en teoría, los Yomus no existen, pero un juez los identificó en los altercados de ese 9 de octubre en Valencia.

«Se ha avanzado mucho. Dentro de los estadios hemos reducido los problemas al mínimo, pero es evidente que tenemos el reto de erradicar la violencia en los alrededores de los campos», explica Alfredo Lorenzo, director de integridad y seguridad de la LFP (Liga de Fútbol Profesional), el organismo que se ha puesto al frente de la lucha contra la violencia con una política de insistencia traducida en denuncias constantes y en, como este jueves, personarse como acusación particular en el caso del apuñalamiento en las cercanías del campo del Atlético.



Una muerte y el silencio

No comparte esa visión Esteban Ibarra, presidente del Movimiento contra la Intolerancia. «Claro que hay un repunte de los ultras. Cuando hay una muerte como fue la de Jimmy, los ultras se sumergen y esperan a que vuelva la aparente normalidad», explica. Cuestionado por esos escasos nueve grupos que aparecen en el listado de Antiviolenia, dice: «La Comisión se pone de perfil y no hace que se cumpla la ley. Trabaja con la información que le facilitan los clubes». Y recuerda que el Observatorio de la violencia, el racismo, la xenofobia y la intolerancia en el deporte lleva «muchos años» sin reunirse porque la Comisión, de quien depende, no lo convoca.



Los clubes insisten en que ellos sólo pueden controlar lo que ocurre dentro de los estadios. Algunos -no todos- han instalado sistemas de identificación biométrica. «Somos los únicos con el sistema de huella dactilar y además pide el DNI a los 4.700 de nuestra grada de animación», insisten desde el Atlético. Pero matizan que, si una organización, en este caso el Frente, es legal -sólo un juez puede ilegalizarla-, no pueden hacer más de lo que han hecho.

Los datos de los pasajeros ya pueden cruzarse con las bases policiales

Fuente: El País
Patricia Ortega Dolz

Tres millones de datos diarios serán enviados en tiempo real por las compañías aéreas

EL PAÍS

El PNR (Registro de Nombres de Pasajeros), una de las herramientas más polémicas contra el terrorismo yihadista, está lista para comenzar a funcionar en España. Cruzará tres millones de datos de pasajeros diarios con las bases policiales del CITCO (Centro de Inteligencia contra el Terrorismo y el Crimen Organizado), donde se ubicará la UNIP (Unidad Nacional de Información de Pasajeros). Allí se almacenarán y transferirán los datos personales de los viajeros enviados por las compañías aéreas. El sistema lo auditará la Agencia de Protección de Datos.

El nombre completo, el teléfono, el correo electrónico, la fecha de reserva del billete de avión, los datos de pago, el itinerario completo del viaje, la frecuencia con la que viaja, la agencia u operador del vuelo, la confirmación de la asistencia al embarque, el tipo de equipaje, el número de asiento, la nacionalidad, el sexo, la fecha de nacimiento, y cualquier cambio en cualquiera de esos campos. Todos esos datos los enviarán las aproximadamente mil compañías aéreas que operan en España a la nueva Unidad Nacional de Información de Pasajeros (UNIP), de reciente creación e instalada en el CITCO.

Allí serán procesados, almacenados, tratados y transferidos por un sistema informático que ha costado cuatro millones de euros y permanecerán operativos seis meses. Después de ese periodo se harán opacos. Y a los cinco años tendrán que ser destruidos. Todo el sistema será periódicamente auditado por la Agencia de Protección de Datos y sus responsables deberán realizar un informe estadístico anual para la Comisión Europea. Así lo recoge la directiva europea del 27 de abril de 2016.

Desde que comenzó su andadura europea en forma de borrador en 2012, el PNR (Registro de Nombres de Pasajeros) ha superado muchos escollos, sobre todo relativos al uso y protección de los datos de los viajeros. Y, casi siempre, los impulsos que ha recibido han venido tristemente

empujados por terribles atentados yihadistas: en Londres, Niza, París, Berlín, Barcelona...

De este modo, una vez que se realice la trasposición interna de la directiva a la normativa española, y se convierta en ley orgánica —puesto que afecta a derechos fundamentales y requerirá la aprobación de la mayoría de los grupos parlamentarios—, los datos que habitualmente recogen las compañías aéreas con fines comerciales podrán ser utilizados con fines policiales, cotejándose con bases de datos nacionales e internacionales, que se encuentran en el CITCO y que nutren constantemente los distintos cuerpos policiales. Dentro de las distintas bases de contraste hay incluso una de documentos falsos.

EL FUTURO VA POR TIERRA Y POR MAR

P.O.D.

La directiva europea deja abierta la posibilidad de que el cruce de los datos de los registros de pasajeros no afecte solo a las compañías aéreas, sino que puedan también proceder de navieras o de compañías ferroviarias y hasta de autobuses, apunta uno de los impulsores del PNR.

“Es el caso de Grecia, por ejemplo”, señala. “Por su geografía, las autoridades ya están trabajando en los registros de pasajeros de las muchas compañías de cruceros que operan en los puertos de sus islas”. El futuro del PNR parece que pasa por el mar y la tierra.



Se usarán para investigaciones relativas a terrorismo, crimen organizado, trata de seres humanos, explotación sexual, corrupción, tráfico de armas, de órganos o de bienes culturales, fraude, blanqueo y falsificación, ciberdelincuencia, delitos contra el medioambiente, homicidio voluntario (o agresión con lesiones graves), secuestro, violación, espionaje industrial... Hasta un total de 26 tipologías delictivas que

recoge la directiva citada podrán motivar las solicitudes de información por parte de los cuerpos y fuerzas de seguridad, policías autonómicas, tribunales y aduanas.

Ya hay un borrador de la ley que ha superado el corte de la Agencia de Protección de Datos, aseguran fuentes del CITCO. Le falta recibir el visto bueno y las aportaciones de los distintos organismos afectados (policiales y judiciales). Y, en teoría, debería estar lista para el próximo 25 de mayo, según las recomendaciones europeas. En cuanto se apruebe la ley, las compañías estarán obligadas a transferir esos datos a la UNIP correspondiente por un canal seguro preestablecido. La transmisión se realiza en tiempo real: entre 24 y 48 horas antes de la salida del vuelo y de nuevo, como confirmación, tras el despegue del avión.



“El sistema está pensado para que todo quede registrado, grabado, cualquier movimiento de información deja un rastro imborrable”, aseguran fuentes del CITCO, donde se ha desarrollado este proyecto que ya funciona en Estados Unidos, Canadá y México.

La idea es que los datos de todos los pasajeros que entren o salgan de España y de la Unión Europea queden archivados para poder ser contrastados en caso de necesidad. A su vez, esa información, podrá ser compartida tanto con países de la UE como con países extracomunitarios, según señala la propia directiva, siempre y cuando las solicitudes respondan a los objetivos de seguridad establecidos.

Según los impulsores de este sistema, el cerebro de los atentados yihadistas de Barcelona y Cambrils del pasado mes de agosto, el imán de Ripoll, Abdelbaki Es Satty, por ejemplo, podría haber sido detectado en uno de sus vuelos de ida y

vuelta de Marruecos porque, con sus antecedentes, estaría incluido en las bases de datos policiales y “habría saltado, habría generado un positivo”, aseguran.

El sistema, que manejará los datos de los 250 millones de pasajeros que se calcula pasan al año por España, es bidireccional. Funciona de manera automatizada con los datos de las compañías aéreas y es incluso capaz de general perfiles de acuerdo con unas características predeterminadas que se soliciten (por ejemplo: mujer, 30 años, viajes a Turquía, nacionalidad francesa). Y a la inversa, se pueden cotejar los datos con una persona ya identificada en el marco de una investigación policial concreta.

RECELOS DE LAS FUERZAS DE SEGURIDAD DEL ESTADO

P.O.D.

El acceso a la información es siempre uno de los caballos de batalla en la colaboración entre los distintos cuerpos y fuerzas de seguridad. Por regla general, todos recelan de todos y muchos de los datos que se comparten se basan en relaciones de confianza, a veces casi personales.

La creación de la UNIP (Unidad Nacional de Información de Pasajeros) y su ubicación en el CITCO ha generado algunas quejas —de momento manifestadas en privado— por parte de los distintos cuerpos, fundamentalmente Policía y Guardia Civil. En ambos casos querrían tener acceso directo a la información de los pasajeros sin pasar por el filtro del CITCO.

Pero la directiva europea establece la creación de una UNIP en cada Estado miembro y su ubicación dentro de una entidad independiente precisamente para salvaguardar al máximo unos datos tan sensibles.

Para aplacar esas protestas soterradas, el CITCO ha propuesto la creación de una base de datos paralela, DELTA, que sea opaca para dicho organismo y que alimenten Policía y Guardia Civil, de manera que solo puedan acceder en caso de que salte un positivo.

Está previsto, en todo caso, que la UNIP arranque con unos 60 funcionarios propios (policías, guardias civiles, o personal de aduanas) y aspira a tener un mínimo de 200 personas, ya que cada caso positivo ha de ser confirmado de manera manual. En teoría, esa oficina funcionará 24 horas al día, siete días a la semana.

EURO DEFENSE ESPAÑA

Fuente: Revista Ejército Nº921 Diciembre 2017
Antonio Nadal Pérez. General de brigada. Artillería. DEM



EuroDefense-España (ED-ESP) es un grupo de estudio y reflexión (*think-tank*), creado, a semejanza de grupos homólogos de Alemania y Francia, y puesto en marcha tras un acuerdo de colaboración entre la Confederación Española de Organizaciones Empresariales (CEOE) y el Ministerio de Defensa, representado por el Centro Superior de Estudios de la Defensa Nacional (CESEDEN), suscrito el 20 de noviembre de 1995.

Desde mayo de 2002 está constituida como asociación sin ánimo de lucro, e inscrita en el correspondiente Registro Nacional de Asociaciones. De acuerdo con sus estatutos, sus fines son:



- Promover el espíritu de Seguridad y Defensa Nacional, y fomentar el conocimiento por la sociedad española de las cuestiones relacionadas con la seguridad y la defensa, así como la presencia y aportación españolas a las necesidades de la seguridad y defensa europea.
- Profundizar en los estudios encaminados al desarrollo de la Política Común de Seguridad y Defensa de la Unión Europea.
- Reflexionar sobre la situación de la industria española de Defensa para apoyar su desarrollo, si es el caso, en colaboración con otros actores especializados, en el

marco de la Política Común de Seguridad y Defensa de la UE.

- Servir de foro de encuentro y discusión a personalidades dedicadas al estudio de las cuestiones antes referenciadas.

Para la consecución de esos fines realiza las siguientes actividades:

- Organiza seminarios, conferencias, coloquios y otras actividades afines.
- Realiza estudios y redacta informes.
- Colabora con otras asociaciones similares de otras naciones.
- Participa en reuniones nacionales o internacionales que se convoquen sobre cuestiones relacionadas con sus fines.

En la actualidad, la Red de Asociaciones EURODEFENSE está formada por las asociaciones de los siguientes 14 países: Alemania, Austria, Bélgica, España, Francia, Grecia, Holanda, Hungría, Italia, Luxemburgo, Portugal, Reino Unido, República Checa y Rumania.



Confederación Española
de Organizaciones Empresariales



Con carácter anual se celebra una *Reunión Internacional de EuroDefense* (RIE) en la que se debaten los trabajos y estudios conjuntos que se están llevando a cabo. La correspondiente a 2017 se hizo en Londres; en Madrid se celebró en el año 2012. También con periodicidad anual se celebra un *Consejo de los Presidentes de las Asociaciones Nacionales*, la última se ha celebrado en Viena en 2017; en Madrid se celebrará la correspondiente al 2019.

Con carácter bienal se lleva a cabo una *Reunión de Jóvenes de EuroDefense* que tiene como objetivo reunir a jóvenes europeos, universitarios y cadetes de las academias militares en sus últimos años de carrera, que tienen la oportunidad de intercambiar ideas, opiniones y reflexiones, en un ambiente multidisciplinar, en torno a una temática previamente marcada de interés de la seguridad y defensa europeas. España tuvo el honor de organizar la reunión del año 2013, que reunió a 70 jóvenes europeos en la Academia de Infantería de Toledo donde debatieron en torno al tema «La Defensa de Europa: Pasado, Presente y Futuro». Como consecuencia del éxito de aquella reunión, *EuroDefense* España recibió el pasado año 2016, el premio *European Award for Citizenship, Security and Defence* que anualmente concede la Asociación *Civisme Défense Armées Nation* (CiDAN), y la *Inter-Parliamentary European Security and Defence Association* (ESDA), con el apoyo de la Asamblea Parlamentaria del Consejo de Europa.

Los componentes de *EuroDefense* España son oficiales superiores de los tres ejércitos, en situación distinta al servicio activo, embajadores, empresarios o profesores universitarios, aunque está abierto a otros profesionales. La participación es a nivel personal, con carácter voluntario y sin ningún tipo de remuneración económica.

La Unión Europea se encuentra en un momento crucial en el desarrollo de su Política Común de Seguridad y Defensa. El ingreso de nuevos Estados miembros a partir de 1991 ha producido unos cambios geopolíticos que, junto con la evolución de los acontecimientos en áreas del Mediterráneo y Oriente Medio, perfilan un entramado dentro del cual España puede y debe jugar un papel fundamental de carácter geoestratégico, económico y militar.



Banderas nacionales de los países integrados en la Red de Asociaciones EURODEFENSE

En este contexto, entre los principales objetivos de ED-ESP está el estudio y el análisis de cuestiones relacionadas con la Defensa Nacional y Europea, siendo uno de los aspectos más destacados el establecimiento de lazos de colaboración con entidades similares en el ámbito fundamentalmente europeo. Todo ello cimentado en valores y principios como la democracia, la solidaridad, la responsabilidad y el respeto por la dignidad humana.

Uno de los sectores fundamentales en el campo de la Seguridad y Defensa es el de la industria de defensa, sector estratégico con un claro efecto multiplicador en la innovación,

el crecimiento y el empleo. Entre las líneas de actuación prioritarias de ED-ESP está la de aprovechar la estructura internacional de las Asociaciones de *EuroDefense*, que engloba a las 14 naciones europeas integrantes de la misma, para defender los intereses de la industria española de Defensa, apoyando a nuestras empresas ante instituciones nacionales e internacionales.

El recorrido de ED-España, desde su creación, ha estado marcado por una activa participación tanto en reuniones como en trabajos individuales o colectivos, con el resto de las asociaciones del grupo *EuroDefense*, cuyos resultados se han materializado en una serie de documentos que, una vez consensuados, se han elevado al Consejo Europeo y a las autoridades españolas competentes en estos campos, enfocados en distintos aspectos de la Política de Seguridad y Defensa Europea.



Las amenazas a la seguridad europea y a nuestra seguridad son hoy en día más diversas, menos visibles y menos predecibles que nunca y a esas amenazas, junto con la diversificación de riesgos, sólo podrá hacerse frente con órganos de decisión eficaces, con fórmulas de acción multilaterales y con el esfuerzo de asociaciones como la nuestra.

ED-ESP cree que, el éxito de estas acciones y la credibilidad de los planteamientos que se adopten, dependerán básicamente de las capacidades propias, debiéndose establecer prioridades, valores y estrategias que sean las más adecuadas para contrarrestar vulnerabilidades y para fortalecer el papel que España desempeña actualmente en el complejo entramado de la seguridad y la defensa europeas.



Reunión de Jóvenes de EuroDefense. Academia de Infantería. Toledo, 2013

Análisis sobre dispositivo de seguridad para la copa mundial de fútbol 2018 en Rusia

Fuente: GIASP (Observatory of Strategy and Intelligence)

Marta G^a Outón



Naturaleza y peculiaridades: Evento deportivo de acogida mundial, con amplio despliegue de servicios y con una agenda en diversas geolocalizaciones a nivel nacional y tiempos con una preparación y anunciamento de más de un año de antelación para su organización, exposición y patrocinio.

- **Fases:** Primera fase (Septiembre-Octubre 2017)/ Segunda fase (Noviembre 2017)/ Tercera Fase (Copa Mundial de la FIFA – Rusia, 14 de Junio al 15 de Julio).
- **Equipos participantes:** Rusia, Alemania, España, Croacia, Inglaterra, Polonia, Serbia, Suiza, Bélgica, Dinamarca, Francia, Islandia, Portugal y Suecia (9 + 4).
- **Lugar de celebración:** Moscú, San Petersburgo, Ekaterimburgo, Kaliningrado, Nizhni Nóvgorod, Kazán, Saransk, Sochi, Rostov del Don, Volgogrado y Samara.

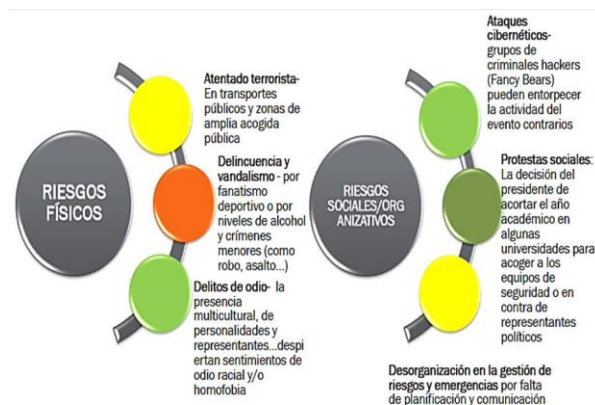


1. Análisis de riesgos:

- **Protección de personal VIP y clientes corporativos:** La agenda deportiva y/o política condiciona el movimiento de personal vinculado a la afición o a la administración pública que obliga a una exhibición pública mayor de lo

normal que pueda dejarles vulnerables a posibles ataques de odio o terrorismo.

- **Violencia y enfrentamientos de odio entre los seguidores y a colectivos:** La presencia multicultural en actos como estos en Rusia despiertan sentimientos de odio racial y/o homofobia, como por ejemplo, hacia personas de origen asiático y africano.
- **Actos de delincuencia y vandalismo organizado:** Los actos de violencia organizada suelen dirigirse contra seguidores del deporte con tendencia a responder (por fanatismo) o por sus habituales niveles de alcohol (como los británicos). Por otro lado, crímenes menores (como robo, asalto...) puede multiplicarse ante la llegada masiva de extranjeros para el evento, sobre todo teniendo lugar en los transportes públicos o conglomerados de turistas.
- **Atentado terrorista en transportes públicos y zonas de amplia acogida pública:** Rusia ya ha sufrido anteriores ataques terroristas, en la zona de Moscú y San Petersburgo al padecer una importante insurgencia en el área de Chechenia y por su política exterior en Oriente Medio. Hasta ahora, este tipo de eventos atrae bastante la posibilidad de un atentado terrorista, al favorecer su publicidad e impacto.
- **Ataques cibernéticos:** En Rusia operan varios grupos de criminales hackers (como los Fancy Bears) que pueden entorpecer la actividad del evento y buscar acceder a la información de los equipos contrarios.
- **Protestas sociales:** La decisión del presidente de acortar el año académico en algunas universidades para acoger a los equipos de seguridad en las instalaciones ha provocado algunos descontentos entre estudiantes universitarios, que se han movilizado en protesta.



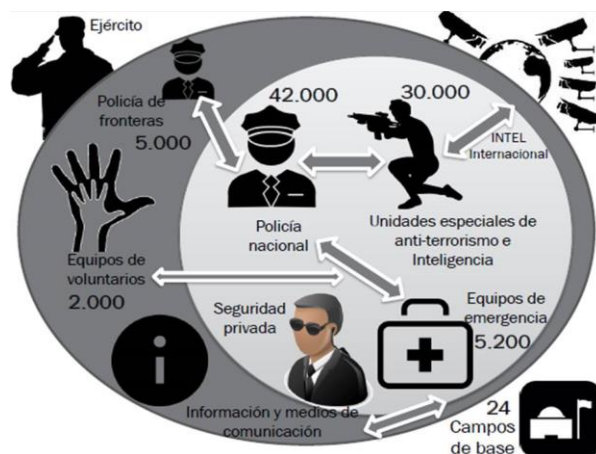
2. Análisis de amenazas: Amenaza predominantemente terrorista, de ataques indiscriminados y de ataques contra personalidades del deporte, así como infraestructuras clave. Posible inspiración de acciones violentas por colectivos o individuos aislados.

- **Amenazas del grupo terrorista Daesh o del movimiento insurgente islámico en Chechenia** de la llegada de un posible atentado terrorista durante el mundial. Amenazan directamente a personalidades, infraestructuras y llaman a ataques indiscriminados.
- El grupo terrorista difundió montajes en los que se ve a uno de sus miembros cerca de varios estadios donde se disputarán partidos del mundial y de las ciudades en las que se celebrará el evento.
- Fotos trucadas por Daesh en los que se puede ver a reconocidos jugadores de fútbol heridos o cautivos, a destacar la selección española. Los muestran capturados por el grupo terrorista y con el traje de preso de Guantánamo utilizado durante sus ejecuciones públicas.
- Lugares sensibles a amenaza: estadios, ciudades de acogida del evento (11), medios de transporte, sitios de entrenamiento de los deportistas, estaciones de transporte (autobuses, metros, aeropuertos, carreteras...).

3. Organizaciones implicadas:

- **EMPRESAS PRIVADAS DE SEGURIDAD** (como ETS-GLOBAL RISK): Presenta una amplia experiencia para la gestión de la seguridad de grandes eventos en Rusia, con anterior presencia en otros mundiales de fútbol (como el de Rio 2016 y Brasil FIFA 2014). Ofrece amplio elenco de personal, vehículos, personal local, traductores y transporte de seguridad. La seguridad privada ofrece una atención especializada y peculiar para necesidades particulares que se escapan a la respuesta administrativa pública y su agenda más general.
- **FUERZAS DE SEGURIDAD ANTITERRORISTAS Y UNIDADES DE INTELIGENCIA:** Con el fin de prevenir y responder ante posible amenaza terrorista (en los alrededores de los estadios, zonas turísticas y en los transportes públicos). Estas fuerzas de seguridad tendrán que operar con un correcto sistema de comunicación y en colaboración/comunicación, con una distribución e información adecuada de competencias, con las fuerzas de seguridad locales y de la Guardia Nacional. Justamente en este grupo de seguridad es fundamental la colaboración internacional en materia de información e inteligencia para el seguimiento y detención de posibles amenazas terroristas.
- **FUERZAS DE SEGURIDAD NACIONALES Y LOCALES:** Para el control de actos vandálicos y el orden público en los accesos a los estadios, áreas turísticas y de transporte con un despliegue de patrullaje y vigilancia.

- **EQUIPOS DE EMERGENCIAS** (contra incendios): Será necesaria la gestión y cooperación entre todos los servicios de emergencia para atender a las necesidades en caso de un incidente. Antes de su despliegue será necesario entonces un entrenamiento reglado ante posibles emergencias durante el evento.
- **EQUIPOS DE VOLUNTARIOS:** Voluntarios de emergencias (médicos, enfermeros, de vigilancia, control de alcoholemia, transporte, comunicación e información...), así como traductores y de acomodamiento, que ayuden en la acogida y seguridad de los asistentes al evento. Para la FIFA 2018 en Rusia se contará con al menos 15.000 voluntarios.
- **EQUIPOS DE MEDIOS DE COMUNICACIÓN E INFORMACIÓN:** Ante un evento semejante, habrá un despliegue de medios de comunicación, nacionales e internacionales.



4. Evaluación y propuestas de acción:

- **“FAN ID”:** es una tarjeta que tiene los datos personales de su propietario, foto, código de barra y sensor. Necesario para entrar a los estadios y que solo obtendrán quienes compren las entradas. Es gratuito y se debe tramitar con anterioridad a viajar a través de la página web fan-id.ru.
- **PASAPORTE DE AFICIONADO:** Los propietarios del pasaporte de aficionado pueden ingresar a Rusia 10 días antes del comienzo del mundial sin necesidad de visado y quedarse en el territorio ruso hasta 10 días después de culminado el torneo deportivo.
- **OPERADORAS DE WIFI PARTICULARES:** Acceso a internet de forma privada para que el personal de los equipos puedan evitar la vulnerabilidad a ataques cibernéticos accediendo a internet público.
- **CENTRO DE INFORMACIÓN:** Centros de información estacionados en los alrededores de los estadios y en sus accesos para facilitar necesidades de información para los visitantes y seguidores de la afición, no sólo en relación al evento, sino también a información clave de seguridad, emergencia y movilización, así como en las responsabilidades (y penalidades) cívicas.

- **PIVOTES DE SEGURIDAD Y DE DETENCIÓN DE ATENTADOS:** Como se ha ido implantando en otras ciudades europeas, levantar pivotes para la detención de atentados con el empleo de vehículo en las zonas peatonales y de tránsito turístico, así como para las inmediaciones del estadio.
- **PROTECCIÓN DE PERSONAL:** Opción de protección cercana para personal VIP, colectivos sociales o personal de la organización del evento. Su protección sería un 24/7 para atender en cada momento y lugar, en constante comunicación con el servicio de protección.
- **SEGURIDAD EN TRANSPORTES:** Servicios de transporte de especial seguridad para movilizarse por Rusia (ya que el evento tiene lugar en al menos 11 lugares del país y para facilitar los intereses particulares y de turismo de los visitantes).
- **UNIDADES DE INTELIGENCIA Y SISTEMAS DE VIGILANCIA, CONTROL DE FRONTERAS:** Es importante la gestión y la colaboración en el seguimiento, análisis y detención de posibles amenazas terroristas y violentas, con la colaboración de otras agencias europeas y nacionales, que faciliten la identificación y neutralización.
- **PANFLETOS DE INFORMACIÓN** junto con documentación, **FIRMA DE RESPONSABILIDADES Y ANUNCIACIÓN mediática:** La comunicación previa de las responsabilidades del ciudadano y las penalidades en

caso de cometer delito es fundamental para exponer las respuestas jurisdiccionales y de seguridad a las que se pueden ver sometidos aquellos que atentan contra la seguridad y el bienestar de los demás, así como de las instalaciones y propiedades del lugar de acogida.

- **CONCIENCIACIÓN DE LA AMENAZA/EMERGENCIAS Y MEDIDAS DE SEGURIDAD:** Es importante la información previa y en el durante del evento de la necesidad del despliegue de seguridad, informando de las posibles amenazas, riesgos y emergencias, para hacer partícipe al ciudadano del sistema de seguridad y de emergencia, así como de las respuestas y actuaciones que se deben llevar a cabo de acuerdo a la organización y agenda de seguridad.

Seguridad física-vial	<ul style="list-style-type: none"> • Comunicación e info: Información previa y en el evento y la necesidad del despliegue de seguridad, informando de las posibles amenazas, riesgos y emergencias, para hacer partícipe al ciudadano del sistema de seguridad y de emergencia y de las respuestas y actuaciones que se deben llevar a cabo según la agenda de seguridad. • Seguridad en transportes y lugares públicos: Servicios de transporte y escolta de especial seguridad para movilizarse por Rusia (ya que el evento tiene lugar en al menos 11 lugares del país y para facilitar los intereses particulares y de turismo de los visitantes) y patrullaje y vigilancia de zonas turísticas y de alta densidad. • Firma de responsabilidades: en caso de cometer delito para exponer las respuestas jurisdiccionales y de seguridad a las que se pueden ver sometidos aquellos que atentan contra la seguridad y el bienestar.
Seguridad ante amenaza yihadista	<ul style="list-style-type: none"> • FAN ID: es una tarjeta que tiene los datos personales de su propietario, foto, código de barra y sensor. Necesario para entrar a los estadios y que solo obtendrán quienes compren las entradas. • Pivotes anti-atentados: Como se ha ido implantando en otras ciudades europeas, levantar pivotes para la detención de atentados con el empleo de vehículo en las zonas peatonales y de tránsito turístico, así como para las inmediaciones del estadio. • Control de fronteras e INTEL: gestión y la colaboración en el seguimiento, análisis y detención de posibles amenazas terroristas y violentas, con la colaboración de otras agencias europeas y nacionales, que faciliten la identificación y neutralización.
Seguridad privada-personal	<ul style="list-style-type: none"> • Plataformas wifi privadas: Acceso a internet de forma privada para que el personal de los equipos puedan evitar la vulnerabilidad a ataques cibernéticos accediendo a internet público • Centros de información: estacionados en los alrededores de los estadios y en sus accesos para facilitar necesidades de información para los visitantes y seguidores de la afición, no sólo en relación al evento, sino también a información clave de seguridad, emergencia y movilización, así como en las responsabilidades (y penalidades) cívicas. • Guardaespaldas: Opción de protección cercana para personal VIP, colectivos sociales o personal de la organización del evento. Su protección sería un 24/7 para atender en cada momento y lugar, en constante comunicación con el servicio de protección.



Queremos recordarte nuestra nueva herramienta de información inmediata y constante del sector, y para todos nuestros Socios y Amigos, a través del Twitter, nos encontrareis aquí: http://twitter.com/ADSI_ES




El foro Davos lanza un Centro Global para la Ciberseguridad a partir de marzo

Fuente: Agencia EFE



El Foro Económico Mundial anunció hoy la creación de un Centro Global para el Ciberespacio, que estará operativo a partir de marzo y con el que pretende fomentar desde Ginebra la colaboración pública-privada en la lucha contra las amenazas cibernéticas.

El director gerente del Foro, Alois Zwinggi, explicó en una rueda de prensa que "claramente la ciberseguridad se ha convertido en uno de los temas más importantes del mundo", ya que el coste de los cibercrímenes ascienden globalmente a 500.000 millones de dólares cada año, según dijo.

La ciberseguridad "afecta a todos los aspectos de la sociedad, incluido el crecimiento económico", recalcó, y dijo que el Foro ve, como organización internacional, una "clara necesidad para una mejor cooperación" entre el sector público y privado.

El Foro Económico Mundial, con sede en Ginebra, dijo, "está comprometido con hacer el ciberespacio más robusto y resistente", a través de la búsqueda de soluciones comunes.

El centro se centrará en cinco áreas, pero quiere seguir implementando y aprovechando foros e iniciativas actuales.

En concreto, el Foro de Davos quiere establecer un "depósito" para la información cibernética, ya que "es crucial que el sector público y el privado compartan datos globalmente, señaló Zwinggi.

El Foro Económico Mundial también pretende generar y aportar oportunidades educativas en ciberseguridad, especialmente en países con mucho potencial para reforzar su defensa.

Además, la organización quiere elaborar recomendaciones para marcos reguladores en este campo y definir el futuro de escenarios en materia de ciberseguridad.

El centro estará ubicado en Ginebra y operativo a partir de marzo, dijo Zwinggi, y aunque formará parte del Foro Económico Mundial, tendrá su propia organización e infraestructura.

Los miembros serán compañías globales de industrias que más se ven impactados por las amenazas cibernéticas y gobiernos del G20 y otros países relevantes además de organizaciones internacionales.



El director de Europol, Rob Wainwright, calificó la creación del Centro de un paso "importante" más en torno a la lucha contra las amenazas cibernéticas, y explicó que de lo que él puede ver en todo el mundo, y especialmente en Europa, -donde su organización acoge el Centro Europeo contra el Cibercrimen- "las amenazas se está convirtiendo en más complejas, desafiantes y más grandes".

Recordó que hay unos 4.000 ciberataques de virus ransomware, impulsados por el "abuso criminal de monedas virtuales".

Wainwright mencionó específicamente el caso en mayo pasado del ataque del virus "WannaCry", que afectó a servicios públicos y empresas en gran parte del mundo, al bloquear ordenadores y exigir un rescate de 300 dólares (254 euros).

"Lo que hemos visto son robos de datos que impactan a miles de millones de usuarios", y hay una tendencia de ataques hacia servicios cruciales, estando el sector bancario en la primera línea de fuego de los criminales, sostuvo.

Cuarteles militares secretos hechos públicos por las pulseras deportivas

Fuente: La Vanguardia
 Álex Barredo

Militares, espías y funcionarios que mantienen activa y pública su ubicación en plataformas deportivas desvelan o confirman la presencia de lugares que estarían mejor secretos



Strava es una plataforma social de atletismo y deporte que permite tener un historial y compartir tus entrenamientos. Desde su fundación hace casi una década ha permitido a ciudadanos de todo el mundo, desde “corredores de domingo” a atletas olímpicos tener mejores datos de su evolución. Solo necesitas un smartphone, una pulsera inteligente o un reloj inteligente compatible, y a correr. O andar, o montar en bici. Desde un punto de vista de pájaro, **sirve para identificar las zonas más populares para correr o montar en bicicleta.**

Precisamente su principal ventaja es también un agujero de seguridad. Muchos de los usuarios de Strava envían consistentemente su localización a sus servidores. Unos datos que son luego expuestos de forma pública pero anónima. En principio nadie puede saber que eres tú el que está corriendo dando vueltas alrededor del parque que rodea tu casa. El problema reside cuando las localizaciones deberían permanecer secretas, o cuando la actividad de los residentes de áreas concretas **queda expuesta porque nadie más podría estar haciendo deporte en esa zona.**

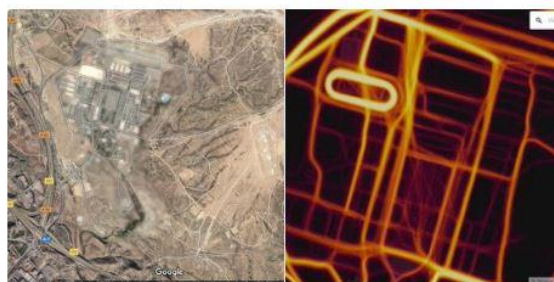
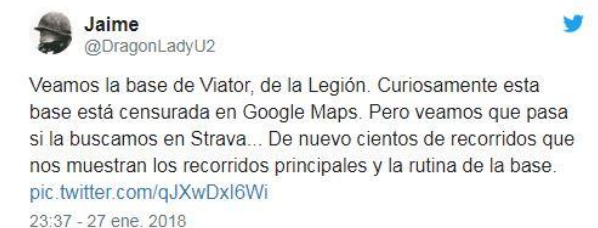
soldados entrenando con la pulsera activada, oficinistas entrando y saliendo de edificios que no albergan personal oficialmente y miembros de agencias gubernamentales revelando las rutas más concurridas en zonas de acceso restringido.

Tobias Schneider, un analista especializado en Oriente Medio, ha publicado las rutas de entrenamiento de varios enclaves militares de Estados Unidos en Irak o Afganistán, del ejército francés en Níger. Incluso cuarteles oficialmente no reconocidos por fuerzas internacionales en Siria, tanto rusas como estadounidenses.

Mirando a España, un análisis superficial de los lugares más vigilados no encuentra nada especialmente relevante. Nadie entrando y saliendo constantemente de las oficinas del CNI en Madrid. Sí aparecen diferentes rutas obvias alrededor del Palacio de la Moncloa o del Palacio de la Zarzuela, pero ninguna respectivamente identificable a ninguna persona, al consistir en trazos múltiples más que probablemente realizados por miembros del servicio y funcionarios en su día a día.

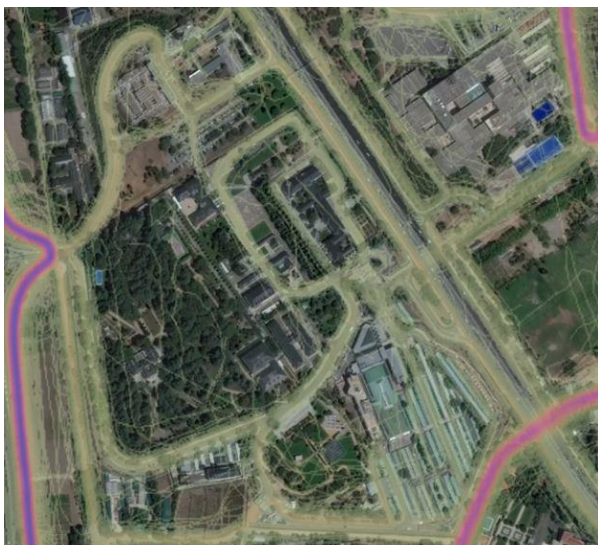


9 128 304



2 21 37

De esta forma, zonas militares, enclaves de inteligencia o puestos avanzados en zonas de guerra quedan revelados por

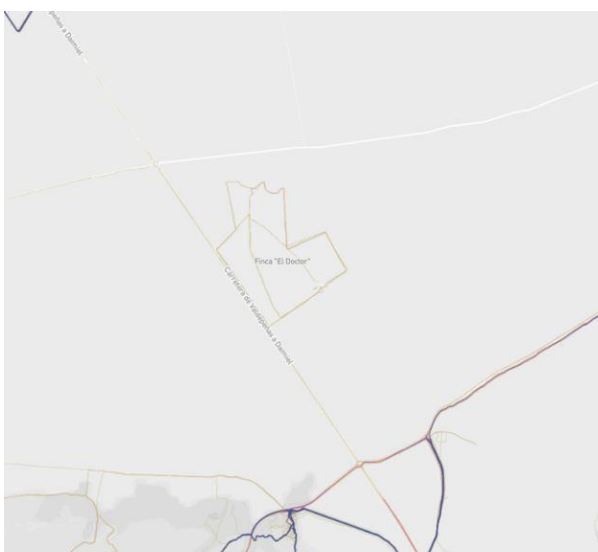


Palacio de Moncloa en Strava (Strava)



Mapa de actividad de Barcelona en Strava (Strava)

Volviendo al CNI, aparecen ligeras líneas —indicando poca popularidad o repetición— en su supuesto centro de entrenamiento de nuevos reclutas en Ciudad Real. La conocida finca “El Doctor” es una residencia donde el servicio de inteligencia español realiza duras pruebas físicas, intelectuales y psicotécnicas a los recién alistados.

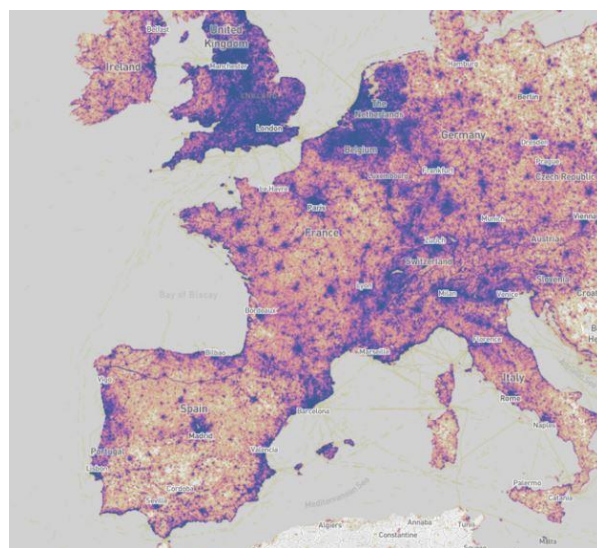


Finca 'El Doctor' de entrenamiento del CNI en Ciudad Real (Strava)

En bases militares conocidas, sirve para identificar cuáles de sus oficios son los más visitados. Este tipo de datos quizá no sean más que anecdóticos como evaluación para agencias de inteligencia o cuerpos policiales, pero cruzados con datos obtenidos por otros medios como los datos de antenas telefónicas o con datos solicitados vía judicial a plataformas digitales, puedan crear un rastro claro de la actividad de una persona o personas concretas.

Estas rutas no son únicas en tierra, también sobre el mar pueden verse rutas de entrenamiento, zonas de pesca claras cercanas al litoral, las direcciones constantes de los ferrys o misteriosos trazados en alta mar. ¿Gente entrenando en la cubierta de un crucero? ¿Marineros de un submarino emergido temporalmente? ¿Trazados repetidos en la noche por los narcotraficantes? Quién sabe, pero **están reflejados en los servidores de Strava**.

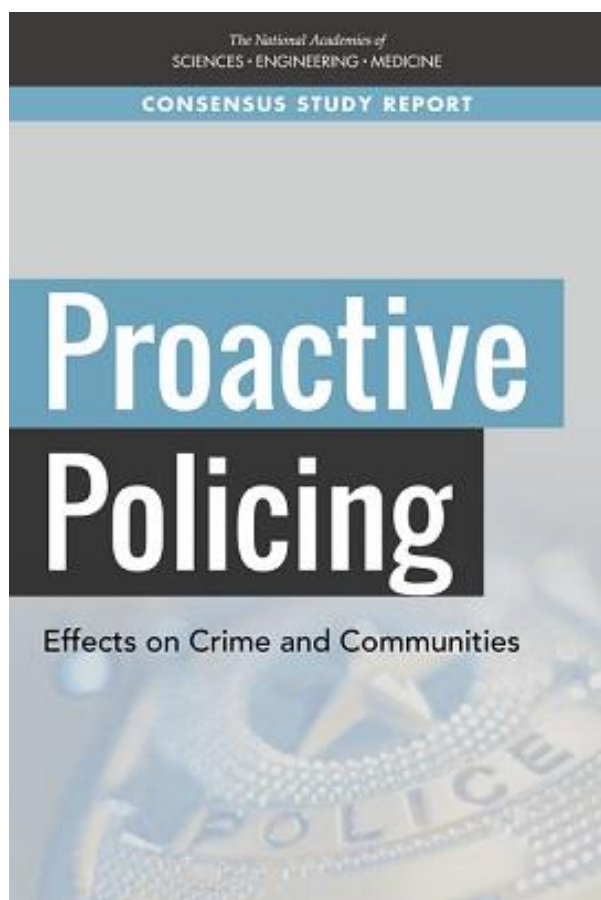
Tomando la vista de pájaro a un nivel más alto, es quizá curioso pero poco sorprendente, que el Camino de Santiago sea rápidamente obvio en un mapa de Europa. El motivo es claro, con miles de fieles recorriendo la ruta cada año, la ruta jacobea permanece inmortalizada como si de un sendero de pequeñas hormigas se tratase.



Camino de Santiago a la vista en un mapa de Europa con Strava (Strava)

Los estrategias policiales proactivas ¿son útiles?

Fuente: Notes de Seguritat



La actuación policial proactiva puede ser entendida como “las estrategias de actuación policial que tienen como uno de sus **objetivos la prevención o la reducción de la delincuencia y los desórdenes**, y que no son reactivas en el sentido de prestar la atención de manera primaria a descubrir la delincuencia que se está produciendo o investigar o responder a los delitos una vez ya se han cometido”. Esta es la definición que se toma como referencia en el libro *Proactive Policing: Effects on Crime and Communities*, publicado por las National Academies of Sciences, Engineering and Medicine de los EE.UU. en noviembre de 2017.

El libro es el resultado de una investigación realizada por un comité científico formado por sociólogos, criminólogos, juristas y miembros de cuerpos de seguridad que pretendía revisar las evidencias y debatir sobre las carencias en los datos y la metodología sobre cuatro aspectos de la **actuación policial proactiva en el combate contra la delincuencia**:

1. Los efectos o las diferentes formas como se implementa

2. Si se aplica de una forma discriminatoria
3. Si se utiliza de acuerdo con las leyes
4. La reacción de la comunidad a esta estrategia de actuación

Para hacerlo, han establecido cuatro aproximaciones diferentes sobre la actividad policial proactiva: basada en el espacio, de resolución de problemas, centrada en las personas y basada en la comunidad. Cada una de estas aproximaciones tiene definidos sus propios modelos lógicos de prevención de la delincuencia, estrategias proactivas, objetivos primarios y vías principales para alcanzar sus objetivos, que se resumen en la siguiente tabla:

	Aproximación basada en el espacio	Aproximación de resolución de problemas	Aproximación centrada en las personas	Aproximación basada en la comunidad
Modelo lógico para la prevención de la delincuencia	Capitalizar la evidencia de la concentración del delito en sitios micro-geográficos	Utilizar una aproximación de orientación al problema, que busca identificar problemas como patrones a través de hechos delictivos y, posteriormente, identificar las causas de estos problemas	Capitalizar las fuertes concentraciones de delitos entre una pequeña proporción de la población criminal	Capitalizar los recursos de las comunidades para identificar y controlar la delincuencia
Estrategias policiales	Policía de puntos calientes; policía predictiva; sistemas de video-vigilancia (CCTV)	Policía orientada a los problemas; policía de terceras partes; partenariados proactivos	Detenciones dirigidas; programas de multirreincidentes; paros y cacheos	Policía orientada a la comunidad; policía de procedimiento de justicia; policía de ventanas rotas
Objetivo primario	Prevenir la delincuencia en pequeños espacios	Resolver problemas recurrentes para prevenir la delincuencia futura	Prevenir y disuadir delitos concretos centrándose en los delincuentes conocidos	Mejorar la eficacia colectiva y la colaboración de la comunidad con la policía
Puntos principales para conseguir el objetivo	Identificar los puntos calientes donde se concentra la delincuencia y aplicar estrategias centradas en estos sitios	Escanear y analizar problemas criminales, identificar soluciones y valorarlos (modelo SARA)[1]	Identificar a los delincuentes conocidos con una tasa de hechos cometidos y aplicar estrategias sobre estos delincuentes específicos	Desarrollar estrategias que incorporan la comunidad o cambiar la manera como la policía interacciona con los ciudadanos

Fuente: National Academies of Sciences, Engineering, and Medicine (2017, pág. 5-2)

El informe ha encontrado evidencias que, como mínimo a corto plazo, **muchas prácticas de policía proactiva tienen éxito en el objetivo de reducir la delincuencia y el desorden**, sin estropear las relaciones entre la policía y la comunidad. No obstante, algunas carencias en la investigación realizada hacen que no se puedan valorar otras cuestiones importantes, como la legalidad de los procedimientos policiales o las conductas discriminatorias por motivos raciales. Tampoco se han podido comprobar los efectos de este tipo de estrategias policiales a largo plazo o aplicadas en un ámbito mayor que el local.

Protección de datos, ¿qué novedades se avecinan?

Oficina de Seguridad del Internauta

Una vez más nos hacemos eco del Día Europeo de la Protección de Datos, que como cada 28 de enero, se celebra a nivel mundial. Este año, desde la Oficina de Seguridad del Internauta recopilamos las principales novedades que se avecinan entorno a esta temática y que afectarán directamente a los usuarios, ya que como muchos sabréis, en apenas cuatro meses comenzará a aplicarse un nuevo reglamento en Europa conocido como RGPD.

¿Sabíais que existe actualmente en España una ley que se encarga de velar por nuestros datos privados? Pues sí, se conoce como Ley Orgánica de Protección de Datos, LOPD, y su objetivo es garantizar y proteger las libertades públicas y los derechos de mantener la intimidad y el honor personal y familiar en España. ¿Esto en qué se traduce? Si alguna empresa o servicio (proveedor) nos solicita datos personales, debe informarnos detalladamente de aspectos como los siguientes:

1. Para qué van a utilizarlos.
2. Qué tratamiento les darán, cómo los van a proteger.
3. Cómo podemos ejercer nuestros derechos ARCO (Acceso, Rectificación, Cancelación, Oposición) al tratamiento de los datos y solicitar, si lo consideramos oportuno, su retirada si creemos que un proveedor está ofreciendo indebidamente información sobre nosotros.

Por tanto, si queremos saber cuál va a ser el uso que se dará a nuestros datos privados, debemos pararnos a leer los "términos y condiciones" y "políticas de privacidad", incluidos los de los servicios online, por muy pesados y tediosos que nos parezcan antes de marcar la casilla de aceptación de los mismos, ya que en ellos deberán estar detallados todos los puntos indicados anteriormente.



Facebook's Privacy Principles

Facebook was built to bring people closer together. We help you connect with friends and family, discover local events and find groups to join. We recognize that people use Facebook to connect, but not everyone wants to share everything with everyone – including with us. It's important that you have choices when it comes to how your data is used. These are the principles that guide how we approach privacy at Facebook.

We give you control of your privacy
You should be able to make the privacy choices that are right for you. We want to make sure you know where your privacy controls are and how to adjust them. For example, our audience selector tool lets you decide who you share with for every post. We develop controls based on feedback from around the world.

We help people understand how their data is used
While our Data Policy describes our practices in detail, we go beyond this to give you even more information. For example, we include education and tools in people's day-to-day use of Facebook – like ad controls in the top right corner of every ad.

Ya lo avanzábamos en publicaciones anteriores en nuestro blog, este 25 de mayo comenzará a aplicarse el nuevo Reglamento General de Protección de Datos (RGPD) que sustituirá a la actual normativa. Dicho reglamento, que entró en vigor el 25 de mayo de 2016, está teniendo un periodo de adaptación de dos años, periodo para que las empresas y organizaciones adapten sus términos y condiciones así como den a conocer estos cambios a sus usuarios. Este reglamento firmado desde el parlamento europeo, recoge los derechos y libertades que nos amparan sobre la protección de nuestros datos dentro de la Unión Europea. Está basado en la responsabilidad activa del tratamiento de los datos por parte de las organizaciones y empresas. La estrategia que sigue es prevenir infracciones

antes de que ocurran, protegiendo nuestros datos por defecto desde el diseño. De este modo las organizaciones y empresas se comprometen en mayor medida a hacer un mejor uso de los datos y a revisar sus avisos de privacidad.

7. ¿Qué implica la responsabilidad activa recogida en el Reglamento?

Uno de los aspectos esenciales del Reglamento es que se basa en la prevención por parte de las organizaciones que tratan datos. Es lo que se conoce como responsabilidad activa. Las empresas deben adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece. El Reglamento entiende que actuar sólo cuando ya se ha producido una infracción es insuficiente como estrategia, dado que esa infracción puede causar daños a los interesados que pueden ser muy difíciles de compensar o reparar. Para ello, el Reglamento prevé una batería completa de medidas:

- Protección de datos desde el diseño
- Protección de datos por defecto
- Medidas de seguridad
- Mantenimiento de un registro de tratamientos
- Realización de evaluaciones de impacto sobre la protección de datos
- Nombramiento de un delegado de protección de datos
- Notificación de violaciones de la seguridad de los datos
- Promoción de códigos de conducta y esquemas de certificación.



Ya queda poco tiempo para que se haga efectivo el nuevo reglamento, por lo que muchas empresas ya están informando a sus usuarios sobre las novedades en sus políticas de privacidad. Es el caso, por ejemplo de Facebook, que aprovechando la celebración del Día de la Protección de Datos, publicó en su blog un artículo con los 7 principios de privacidad con los que quieren ayudar a los usuarios a manejar su propia información de una manera fácil y sencilla.

¿Qué efectos tiene el nuevo reglamento sobre los ciudadanos?

Entre otros, cabe destacar que a partir de la fecha indicada, 25 de mayo de 2018, podremos solicitar que nuestros datos desaparezcan de la base de datos de determinados registros cuando éstos ya no sean necesarios para la finalidad con la que fueron recogidos o cuando éstos hayan sido recogidos de forma ilícita. Además, podremos solicitar que se bloqueen en las listas de resultados de los buscadores enlaces a información obsoleta, incompleta, falsa o irrelevante. Por otro lado, también tendremos derecho a solicitar la recuperación de los datos para poder ser transferidos a otro responsable. Por ejemplo, si tenemos contratado un determinado servicio con una compañía y deseamos cambiarnos a otra, nuestros datos serán transferidos de responsable a responsable a través de las dos compañías dentro de la Unión Europea.

En cualquier caso, para obtener todos los detalles sobre el reglamento, recomendamos visitar la página oficial de la Agencia Española de Protección de Datos, donde hay mucha información al respecto.

Noticias

redacción médica Interior quiere que cada hospital español tenga un director de seguridad

La **Policía Nacional** busca que las autoridades sanitarias asuman en primera persona su **enfoque "proactivo"** ante las **agresiones sanitarias**. De manera paralela a la creación de la figura del interlocutor policial sanitario, tanto a nivel nacional como territorial, se están llevando a cabo reuniones con actores relevantes del sector sanitario para trasladar sus recomendaciones, entre las cuales figura, según fuentes oficiales, el establecimiento de figuras como el **departamento** o el **director de seguridad**.

Según explican estas mismas fuentes, solo un puñado de hospitales disponen en la actualidad de un director de seguridad como tal a nivel nacional. En la Comunidad de Madrid existe este cargo, por ejemplo, en la Fundación Jiménez Díaz o en el Doce de Octubre, además de en el psiquiátrico José Germain; sin embargo, la mayoría de los hospitales y centros de salud subsumen estas funciones en sus órganos encargados de la prevención de riesgos laborales o incluso en los departamentos de mantenimiento.

Para los cuerpos de seguridad, que las instituciones sanitarias contasen con un departamento de seguridad para sus hospitales y centros de salud sería **un paso de gran utilidad**, que seguiría al que ya se ha dado con la creación del interlocutor policial sanitario, ya que permitiría que ambas partes, por un lado el sector sanitario y por otro, la **Policía**, "hablen **un mismo idioma**". De los aproximadamente 180 hospitales públicos españoles, no llegan a 15 los que cuentan con tal departamento de Seguridad, según los datos del Observatorio Integral de Seguridad en Centros Hospitalarios (**Osich**).

Uno de los problemas que se está encontrando la Policía a la hora de luchar contra las agresiones sanitarias es la falta de "cultura de seguridad" en el ámbito sanitario, lo que se traduce en desconocimiento de los límites entre protección y riesgos laborales y en la falta de definición de un plan de seguridad. Ambos problemas se solucionarían con la existencia de un **director de seguridad**, explican estas fuentes, que aclaran que no es necesario que esta figura exista en cada hospital, sino que puede ser autonómica o a nivel de cada área sanitaria.

Esta visión, expresada desde el ámbito policial, coincide con la que mantienen los expertos en seguridad de otros ámbitos. Un repaso a la prensa de ese sector deja claro que hay una percepción generalizada de que los hospitales deberían contar con medidas análogas a otras infraestructuras especialmente sensibles. En un artículo en la revista Seguritecnia, por ejemplo, **Miguel Ángel Peñalba de la Torre**, técnico de gestión de la Seguridad del Hospital Universitario Río Hortega compartía esta inquietud y manifestaba que "tenemos que comunicar a los directivos que la seguridad es básica para realizar la **asistencia de manera más eficaz**".



La Europol lanza la plataforma SIRIUS para facilitar las investigaciones en línea

La plataforma SIRIUS es una solución práctica e innovadora destinada a hacer frente a los retos actuales a que hace frente la aplicación de la ley en las investigaciones en el ámbito de internet.

Los delincuentes que operan en internet cada vez utilizan más herramientas y servicios fácilmente accesibles y creados por otros (el conocido **Crime-as-a-Service**). Eso provoca que **las autoridades policiales se enfrenten a un reto muy complejo** cuando se llevan a cabo investigaciones criminales en línea.

Para hacer frente a este desafío y para dar un mejor apoyo a las investigaciones de los estados miembros de la UE en internet, Europol lanzó oficialmente la plataforma SIRIUS durante una reunión en La Haya en el mes de octubre de 2017.

SIRIUS es una plataforma web segura para los profesionales de la aplicación de la ley que **les permite compartir conocimientos, buenas prácticas y conocimientos técnicos en el campo de las investigaciones de delincuencia** favorecidas por internet, con especial atención a la lucha contra el terrorismo. Su innovador enfoque colaborativo ofrece a los investigadores una plataforma para intercambiar de forma rápida y eficaz conocimientos técnicos, manuales y consejos, así como herramientas para ayudarlos a analizar la información recibida por los distintos proveedores de servicios en línea. La plataforma también aborda otros retos en las investigaciones criminales, como racionalizar las solicitudes a los proveedores de servicios en línea y mejorar la calidad del registro de respuesta.

SIRIUS pretende fomentar el co-desarrollo de herramientas y soluciones que puedan servir de base a investigaciones basadas en internet. Con esta finalidad, Europol organizará una reunión bianual en La Haya, que prevé reunir policías expertos en programación informática para desarrollar conjuntamente herramientas y soluciones comunes.

El impulso político del Foro de Internet de la UE y el trabajo de la Comisión Europea sobre el acceso transfronterizo a pruebas electrónicas, generó que se propusiera la plataforma SIRIUS como una **solución práctica que responde a la demanda de un portal de información y apoyo en línea en el ámbito de la UE**.

La reunión inicial de SIRIUS, celebrada en la sede de Europol, reunió a más de 100 profesionales de 30 países y más de 60 organizaciones diferentes, incluyendo la aplicación de la ley y las autoridades gubernamentales de los estados miembros de la UE y terceros socios, así como representantes de Facebook, Google, Microsoft, Twitter y Uber.

Esta reunión anual de SIRIUS y los acontecimientos bianuales demuestran el compromiso de Europol de estar a la vanguardia de la innovación para **dar apoyo a las investigaciones delictivas que favorece internet**.

Formación



Instituto Internacional de Estudios en Seguridad Global – Fundación Aucal

Oferta Formativa Febrero 2018

Área de Terrorismo, Defensa e Inteligencia

- Máster en Contrainteligencia, Geoestrategia Internacional y Terrorismo Yihadista
- Máster de Historia Militar

SEMINARIOS

- "...Así en la guerra como en la empresa..."
- Los Medios de Comunicación y la Gestión de la Información ante los atentados terroristas

Más Información en el [siguiente enlace](#)



Cursos Especializados de Dirección 2018

Más información y programa en el [siguiente enlace](#)



Oferta formativa de la Escuela de Prevención y Seguridad Integral

La **Escola de Prevenció i Seguretat Integral (EPI)**, adscrita a la Universitat Autònoma de Barcelona, ofrece estudios universitarios en el ámbito de la prevención y la seguridad integral.

Programa en el [siguiente enlace](#)

Legislación



DECRETO 1/2018, DE 9 DE ENERO, POR EL QUE SE REGULA EL REGISTRO DE PLANES DE AUTOPROTECCIÓN DE CASTILLA-LA MANCHA.

PDF de la disposición en el [siguiente enlace](#)



ORDEN HFP/41/2018, DE 23 DE ENERO, POR LA QUE SE PUBLICA EL ACUERDO DEL CONSEJO DE MINISTROS DE 29 DE DICIEMBRE DE 2017, POR EL QUE SE MODIFICA EL ACUERDO GOV/89/2017, DE 4 DE JULIO, POR EL QUE SE APRUEBA LA OFERTA PARCIAL DE EMPLEO PÚBLICO DEL CUERPO DE MOSSOS DE ESCUADRA DE LA GENERALITAT DE CATALUÑA PARA EL AÑO 2017.

PDF de la disposición en el [siguiente enlace](#)

Revistas



Seguritecnia Nº 449. Enero

Nuevo número de **SEGURITECNIA**, con reportajes, entrevistas y artículos, destacando:

- **Editorial:** Año nuevo, leyes nuevas
- **Seguripress**
- **Crónica de la III Jornada de Seguridad en el Transporte Terrestre**
- **Seguridad de las redes y sistemas de información** Por César Álvarez

Enlace: [ver revista digital](#)



Cuadernos de Seguridad Nº 329. Enero

En este número de **CUADERNOS DE SEGURIDAD**, además de las secciones habituales de «Seguridad», «Cuadernos de Seguridad estuvo allí», «Estudios y Análisis», o «Actualidad», el lector encontrará:

- **Editorial:** «Treinta años de servicio al sector».
- **En Portada:** «El sector de la Seguridad ante un mundo globalizado».
- **Entrevistas:** «Enrique Hormigo, presidente de la APDPE».
- **Artículos:** «El sector de la Seguridad afronta en 2018 un año decisivo para su futuro».

Enlace: [ver revista digital](#)



¿Quieres ser Socio de ADSI – Asociación de Directivos de Seguridad Integral?

Para iniciar el proceso de alta como Asociado, envíe un e-mail a secretario@adsi.pro, indicando nombre y apellidos, una dirección de correo y un teléfono de contacto.

En cuanto recibamos su solicitud le enviaremos el formulario de Solicitud de Admisión.

¿Quién puede ser socio de ADSI – Asociación de Directivos de Seguridad Integral?

Puede ser socio de **ADSI**:

- Quien esté en posesión de la titulación profesional de Seguridad Privada reconocida por el Ministerio del Interior (T.I.P. de Director de Seguridad, Jefe de Seguridad, Detective Privado o Acreditación de Profesor de Seguridad Privada).
- Todo Directivo de Seguridad que posea, a criterio de la Junta Directiva de la Asociación, una reconocida y meritoria trayectoria dentro del sector.



La opinión manifestada por los autores de los artículos publicados a título personal que se publican en este medio informativo no necesariamente se corresponde con la de ADSI como Asociación.

Esta comunicación se le envía a partir de los datos de contacto que nos ha facilitado. Si desea cambiar su dirección de correo electrónico dirija su petición por correo postal a "ADSI - Asociación de Directivos de Seguridad Integral", Gran Vía de Les Corts Catalanes, 373 – 385, 4ª planta, local B2, Centro Comercial "Arenas de Barcelona", 08015 - Barcelona, o mediante e-mail a secretario@adsi.pro.

Si o no desea recibir nuestros mensajes informativos utilice los mismos medios, haciendo constar como asunto "DAR DE BAJA". Su petición será efectiva en un máximo de diez días hábiles.