AESCRA Newsletter

AESCRA EN SECURITY FORUM 2025

El pasado 5 de junio el presidente asistió a Security Forum 2025 en Barcelona a impartir una ponencia titulada “Centrales Receptoras de Alarmas, Amenazas y vulnerabilidades. Acciones en marcha para intentar mejorar el contexto legal”. Acudió representando a FES y a AESCRA. Aprovechó para charlar un buen rato con el Comisario Yanguas para insistirle a que por favor se muevan en la UCSP con mayor agilidad en la propuesta de cambio de la INT-316-2011.

ASAMBLEA ANUAL DE UAS

Se celebró el pasado 26 de mayo. Asistieron los 4 asociados de la agrupación: AES, ACAES, AESGA y AESCRA. Propusieron la firma de un código ético , algo inexistente desde su fundación...

Asociaciones fundadoras

AES Asociación Española Empresas de Seguridad

ACAES Associació Catalana d'Empreses de Seguretat

AESGA Asociación de Empresas e Expertos de Seguridade de Galicia

Socio colaborador

AESCRA

ASAMBLEA ANUAL DE UAS

Unión de Empresas de Seguridad

U.A.S.

Unificando criterios en Seguridad Privada.

Se celebró el pasado 26 de mayo. Asistieron los 4 asociados de la agrupación: AES, ACAES, AESGA y AESCRA. Propusieron la firma de un código ético, algo inexistente desde su fundación y que ahora, tras nuestra entrada, vieron conveniente hacer con urgencia sin darnos la oportunidad de participar en su redacción.

Estuvimos de acuerdo con la idea de contar con un código ético, que ya tardaban en tenerlo desde hace tantos años, pero no con un punto del contenido donde obligan a los miembros a no pertenecer a otras asociaciones o agrupaciones sectoriales. Nuestro asesor legal les informó de que esa petición era ilógica e inaceptable, proponiendo textos alternativos que evitasen el conflicto de interés que les preocupaba, pero fueron rechazadas y quedó aprobado por mayoría. Explicaron que no quieren relación alguna con FES ni TECNIFUEGO, asociaciones a las que ahora pertenecemos, por diferencias de criterio en algún asunto y desavenencias pasadas. Ofrecimos mediar para tratar de arreglar esas relaciones pero se negaron en redondo. Así que nuestro presidente les dijo que, dado este giro inesperado de guion, creado exprofeso por nosotros, en la siguiente asamblea general de AESCRA pedirá la aprobación de los asociados para salir de UAS. No obstante, en aras a defender los intereses comunes de nuestros asociados CRAs, estuvieron de acuerdo en que acordemos convenios puntuales para trabajar conjuntamente en asuntos de interés común, empezando por la solicitud de cambio de la INT-316-2011. Cabe destacar que es lo primero que les ofrecimos hace años, celebrar un convenio, y fueron ellos quien vieron mejor que nos incorporásemos a UAS. Mala visión la de unas pocas asociaciones sectoriales que ven en otras a un competidor en vez de un aliado.

AVANCES CON LA MODIFICACIÓN DE LA INT-316-2011

Siguiendo las indicaciones del Secretario General Técnico del Ministerio del Interior, se elevó el documento a las UCSP a primeros de año. Desde entonces estamos haciendo múltiples reclamaciones para que se pongan a trabajar sobre nuestra petición, consensuar el texto y que lo eleven al Ministerio. Una vez ahí, si hiciese falta, pasaremos a la fase de presionar directamente al Ministerio para su publicación a través de CEOE o CEPYME. De momento, los presidentes de FES y AESCRA han solicitado una reunión con Manuel Yanguas para que se muevan. A fecha de elaboración de este boletín, el Comisario nos ha adelantado que una persona de su equipo iba a preparar un cuadro con todas las peticiones que le han pasado las diferentes asociaciones con respecto a esta misma modificación. No somos los únicos que estamos pidiendo lo mismo, lo cual ya nos viene bien, pero es bastante desesperante ver el ritmo que llevan con este asunto en la UCSP. Al parecer el concepto COLABORACIÓN no tiene la misma consideración y urgencia cuando es la Seguridad Privada quien requiere la ayuda de la Pública. No obstante, somos perseverantes y seguiremos insistiendo. De momento, el presidente de FES y el nuestro han acordado una reunión con Manuel Yanguas el próximo 10 de septiembre, no se ha podido poner antes por razones de agenda.

COMUNICACIÓN TELEMÁTICA DE ALARMAS

El 27 de marzo asistimos a la reunión convocada por la Subdirección General de Sistemas de Información y Comunicación para la Seguridad (SGSICS) de la Policía Nacional, donde dieron a conocer el conector informático que han desarrollado para que las CRAs comuniquemos telemáticamente las alarmas a Policía Nacional y Guardia Civil. Es un proyecto que se inició en 2018 y que por fin ve la luz. Será un mecanismo de uso voluntario, quien quiera seguir realizando llamadas podrá hacerlo.

El pasado 8 de abril organizamos un webinar para explicarlo a los asociados de AESCRA y FES, donde sabéis coordinamos su comité de trabajo de CRAs. A fecha de elaboración de este boletín se está reclamando a dicha Subdirección General por qué no se han puesto aun en contacto con las CRAs que les hemos mandado la solicitud.

Centro Tecnológico de Seguridad (CETSE)

El Centro Tecnológico de Seguridad (CETSE) Constituye la sede de la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS)

SGSICS
SUBDIRECCIÓN GENERAL DE SISTEMAS DE INFORMACIÓN Y COMUNICACIONES PARA LA SEGURIDAD

Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS)

Dependiente de la Secretaría de Estado de Seguridad tiene sus funciones asignadas mediante el Real Decreto 207/2024 de 27 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior.

La misión de la SGSICS, es la de proponer, planificar, coordinar, e implantar bases de datos, sistemas de información y sistemas de comunicaciones para su utilización por las Fuerzas y Cuerpos de Seguridad del Estado (FFCCSE), permitiéndoles desempeñar su labor de salvaguarda de los derechos, libertades y seguridad de la ciudadanía de una manera más eficiente y efectiva.
El desarrollo y mantenimiento de aplicaciones de propósito general, incluyendo lo relativo a la transformación digital del Ministerio.

AVANCES CON LAS ALARMAS DE INCENDIO

En TECNIFUEGO ha comenzado la actividad el grupo de trabajo CRI dentro de la Comisión Sectorial de Detección. El grupo lo componen 19 empresas o entidades y lo lidera AESCRA, bien mediante nuestro presidente o en su ausencia el vicepresidente. Se está trabajando en un borrador que va a definir un contexto para la conexión y tramitación de las alarmas de incendio. Se avanza deprisa, se llevan varias reuniones de trabajo, la siguiente será el 25 de junio. Una vez terminado y consensuado el documento, un primer paso será su publicación como anexo a la Guía de TECNIFUEGO de 2021 "Documento Técnico Gestión Remota de Alarma de Incendios. Servicios asociados a Central Receptora de alarmas de Incendio (CRI)". Posteriormente se elevará al Ministerio de Industria.

DOCUMENTO TÉCNICO GESTIÓN REMOTA DE ALARMA DE INCENDIOS
Servicios asociados al mantenimiento

22 de junio de 2021

tecnifuego
Asociación Española de Sociedades de Protección Contra Incendios

OBJETIVO Y ALCANCE

Establecer los requisitos mínimos que deben cumplir las Centrales Receptoras y Gestión de Alarmas de Incendio (CRI), incluyendo criterios de seguridad, continuidad del servicio y calidad de la gestión de señales.

Diferencia claramente entre CRI (alarma de incendios) y CRA (alarma general)

NORMATIVA APLICABLE

Basado en el RIPCI (RD 513/2017) y las normas UNE-EN 54, en particular partes:

EN 54-21: transmisores de alarma y fallo.

EN 54-13: compatibilidad de componentes.

EN 54-2/4/14: controles e instalación.

Además, se incluyen referencias a la Ley de Seguridad Privada y Reglamentos específicos para CRI/CRA

CONCLUSION

El documento define un proceso robusto para que las alarmas de incendio tengan una gestión remota eficiente, segura y normativamente válida mediante CRI. Asegura que, en instalaciones sin vigilancia permanente local, haya una correcta transmisión, verificación y acción inmediata, alineado con las normas UNE-EN 54 y el RIPCI.

ARTICULOS DE PRENSA DESTACADOS

APP PARA LA VIDEOVIGILANCIA EN LA VÍA PÚBLICA

Una APP permitirá activar la videovigilancia a quien se vea en riesgo. El área metropolitana licitará este año un sistema de seguridad público-privado con un coste de 13'9 millones en la ciudad de Barcelona.

Recordad que nuestro asociado colaborador SOFTGUARD tiene este tipo de soluciones que además personalizan y adaptan a cada necesidad o colectivo, también a Ayuntamientos. Contactad con ellos si queréis profundizar en conocer sus soluciones ; el 19 de septiembre tendrá lugar un webinar organizado por AESCRA y SOFTGUARD para profundizar sobre este tipo de soluciones.

https://www.lavanguardia.com/local/barcelona/20250603/10746463/app-amb-permitira-activar-videovigilancia-vea-riesgo.amp.html

¿Qué es la app?

Botón del pánico ciudadano: cualquier persona registrada puede pulsar un botón en su móvil para indicar que se siente en peligro. El sistema geolocaliza al usuario y activa automáticamente todas las cámaras de videovigilancia —públicas y privadas— cercanas

Tecnología y modelo de funcionamiento

Basada en la app M7 Citizen Security, desarrollada por Einsmer (Cornellà), ya en uso en varios municipios pequeños desde hace más de diez años.

La app también permitirá alertas proactivas (tráfico, manifestaciones, cortes de calle) y colaborará en la generación de modelos predictivos para políticas urbanas.

Estado actual del proyecto

Aprobada en junio de 2025 por el AMB.

Próxima licitación antes del verano de 2025.

Previsión de lanzamiento: a lo largo de 2026

Controversia y aceptación

Opiniones divididas: algunos ven la app como una nueva forma de protección ciudadana; otros advierten de riesgos legales y privacidad.

El ayuntamiento de Barcelona presentó alegaciones, especialmente en relación con la edad mínima (14 años) y la legalidad del uso de competencias municipales

En resumen

La APP del AMB será una herramienta de seguridad bidireccional, que permitirá tanto alertar emergencias como recibir avisos oficiales urbanos. Combina tecnología colaborativa, vigilancia predictiva y conexión directa con CCTV. Su despliegue se espera para 2026, siempre sujeto a adaptar la herramienta a los estándares de protección de datos y legitimidad jurídica.

Asociado

Recordad que nuestro asociado colaborador SOFTGUARD tiene este tipo de soluciones que además personalizan y adaptan a cada necesidad, también a Ayuntamientos. Contactad con ellos si queréis profundizar en conocer sus soluciones ; el 19 de septiembre tendrá lugar un webinar organizado por AESCRA y SOFTGUARD para profundizar sobre este tipo de soluciones.

SANCIONES 2024 POR USO DE DATOS BIOMÉTRICOS

Ha costado mucho que las empresas instaladoras de sistemas entiendan el riesgo que supone la implantación de soluciones biométricas en las instalaciones de sus clientes. Los fabricantes y la Covid-19 impulsaron la venta de equipos que hacían del tratamiento facial o de la huella dactilar algo cotidiano y, en apariencia, inofensivo. La implantación del registro de jornada, pasada la pandemia de Covid, supuso una oportunidad para extender este tipo de dispositivos pero el encaje legal de los mismos siempre ha sido muy dudoso. La integración de la identificación biométrica en sistemas de videovigilancia/video analítica , bajo el genérico paraguas de la IA, puede suponer una vuelta de tuerca a este "viejo" problema legal.
A continuación, aunque es algo extenso, por su interés procedemos a difundir un extracto de algunos de los procedimientos sancionadores más relevantes que la AGPD ha abierto en 2024, en relación al uso de datos biométricos (fuente: memoria AGPD 2024)

Sigue siendo muy habitual que este tratamiento se realice con la finalidad de implantar sistemas de fichaje en el entorno laboral, como en el caso del PS/00170/2023 contra CTC Externalización, S.L. En este procedimiento se constatan tres infracciones: una infracción del artículo 13 del RGPD (deber de información) por la que se impone una multa de 200.000 euros, una infracción del artículo 32 del RGPD con una multa de 65.000 euros y, por último, una infracción del artículo 35 del RGPD por la que se impone una multa de 100.000 euros. Además de la multa, impone que, en el plazo de 6 meses, acredite haber procedido al cumplimiento de medidas para asegurar el cumplimiento con la normativa de protección de datos.

PS/00484/2023 contra la Liga Nacional de Futbol Profesional (LNFP). Este procedimiento sancionador se abrió como consecuencia de la presentación de dos denuncias contra la LNFP por la instauración de un régimen de datos biométricos para acceso a los estadios en el sector de la grada de animación. La LNFP exige a los clubes la implantación de la medida, en función de unos fines (el acceso), a una parte del estadio (la grada de animación), con una base legitimadora (consentimiento), y ofertando a los clubes los medios a través de una sociedad de su grupo (SEFPSA, la misma que obligatoriamente por norma ha de aplicar los tornos de acceso).

Tras la tramitación de expediente sancionador se ha probado que LNFP es responsable del tratamiento de las operaciones de tratamiento consistentes en la contratación del sistema de reconocimiento biométrico, para procurar el control de acceso a los estadios de primera y segunda división en relación con la grada de animación, puesto a disposición de los clubes de fútbol y SAD.

Los hechos probados ponen de manifiesto que es la LNFP quien ha decidido tratar datos biométricos para una determinada finalidad, implementar ese sistema y contratarlo, y ponerlo a disposición de los clubes de futbol y SAD, instándoles a su uso. Se estima que la LNFP es responsable del tratamiento, por lo que al configurar dichos datos como exigibles, debió haber efectuado una EIPD del artículo 35 del RGPD.

La multa por infracción del artículo 35 del RGPD, inicialmente prevista en 10.000.000 €, se ha rebajado a 1.000.000 euros tras las alegaciones y documentación aportada por la LNFP a la propuesta de resolución. Se impone una medida correctiva: se estima procedente elevar a definitiva la suspensión temporal que evite la continuación del tratamiento de los datos personales a través del sistema de reconocimiento biométrico para los accesos a la grada de animación de los Clubes y SAD afiliados a la LIGA, en tanto no realice y supere una evaluación de impacto de protección de datos del tratamiento.

También relacionado con el acceso a recintos deportivos encontramos el PS/00482/2023 contra el Club Atlético Osasuna, que se inicia como consecuencia de una reclamación por la implantación de un sistema de Reconocimiento facial (RF) para acceder a su estadio. Antes de la implantación del sistema de reconocimiento facial, contaba con un sistema de acceso basado en la tarjeta de abonado o en su versión de tarjeta de abonado con código QR o tarjeta de abonado en el móvil, sistema que mantuvieron compatibilizándolo con el sistema de reconocimiento facial.
Se examina si cumplen con el triple juicio de proporcionalidad. En la resolución se indica que se produce la infracción del artículo 5.1.c) del RGPD, ya que, se puede conseguir identificar al abonado que accede, pero no se acredita tal necesidad o por qué no se emplea un sistema de verificación, pero se omite la adecuación y pertinencia para la finalidad para la que se requiere. La EIPD no hace valoración alguna del problema que intenta abordar, porque no lo explica, solo ofrece este modo de acceso como voluntario y alternativo al que ya existe y al que se puede volver en cualquier momento. Se impone una sanción de multa de 200.000 euros y se elevan las medidas provisionales a definitivas.
El PS/00432/2023 contra Loro Parque, S.A. se inicia como consecuencia de tres reclamaciones. Los reclamantes, acuden a los parques Loro Parque y Siam Park, pertenecientes ambos al reclamado y reclaman porque al acceder se les ha recogido la huella dactilar, sin ser informados y sin saberlo porque no figura información alguna en las entradas cuando se adquieren. Se sanciona por el artículo 9.1 del RGPD con multa administrativa de 250.000 euros, dado que se recogen datos de todas las personas, de todas las edades. Además, se imponen medidas correctivas.
En el PS/00419/2024 contra el Colegio Notarial de Aragón, se trata de un sistema de fichaje para el control laboral con datos biométricos (huella dactilar). Se imputa una infracción del artículo 9 del RGPD por no contar con una circunstancia que levante la prohibición general del tratamiento de datos biométricos que establece el artículo 9.1 del RGPD y otra del artículo 35 también del RGPD por no superar una evaluación de impacto de datos personales. El importe de la multa es de 10.000 euros. A lo largo del procedimiento se analiza el tratamiento que realiza el Colegio llegando en a la conclusión de que en este caso no actúa en el ejercicio de sus funciones públicas, a pesar de ser una Corporación de Derecho Público.
También en el ámbito laboral, el PS/00414/2023 contra Societat Municipal D'aparcament se inició como consecuencia de una denuncia por la que se ha tenido conocimiento de que se han producido grabaciones a los trabajadores ORA, en el ámbito laboral y sin su consentimiento, a través de una aplicación instalada en los dispositivos de trabajo (PDA) que usan habitualmente. Se imputa una infracción del artículo 5.1.a) del RGPD con una multa administrativa de 40.000 €.
Siguiendo con los procedimientos por el tratamiento de datos biométricos, el PS/00361/2023 contra Cartonajes Bañeres, S.A. se realiza por haber estado utilizando un sistema de reconocimiento facial para el fichaje laboral lo que dio lugar a la presentación de una reclamación en la que también se incluía la falta de respuesta de un ejercicio de acceso. Se imputan las siguientes infracciones con la imposición de las siguientes multas artículo 35 del RGPD, con 200.000 euros; artículo 15 del RGPD, con 20.000 euros. Además, se le da un plazo de 30 días para que acredite haber atendido al cumplimiento del ejercicio del derecho de acceso del reclamante.
Como se observa, el riesgo de sanción en caso de implantación de sistemas biométricos es altísimo en este momento. Existe cierta posibilidad de apertura anunciada por criterios divergentes de otras autoridades nacionales europeas en materia de protección de datos ; ya veremos en el futuro si existe un cambio de criterio de la AGPD motivado, tal vez, por una necesidad de coordinación y/o casación de criterios a nivel europeo. Por el momento, el aviso a navegantes es claro y contundente.

INFORME DE EUROPOL IOCTA 2025

EUROPOL recientemente ha publicado en su página web la edición del informe IOCTA 2025 -Internet Organised Crime Threat Assessment- con el título "Steal, deal and repeat: How cybercriminals trade and exploit your data" mediante el que se analiza el acceso ilegal a los datos personales como paso previo a diversas actividades delictivas en el ámbito de la ciberdelincuencia. A continuación reproducimos el enlace mediante el que pueden descargarse la citada publicación con el correspondiente acceso al informe IOCTA 2025: https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data

Principales Titulares

1. El informe revela la "economía oculta" de los datos robados
Se expone cómo los datos personales y corporativos se han convertido en una mercancía de alto valor en el ciberespionaje y el ciberdelito.

2. La IA generativa potencia los ataques de ingeniería social
El uso de LLMs permite crear mensajes personalizados y engaños más eficaces, mejorando aún más la eficiencia del phishing y otras estafas.

3. El crimen-as-a-service acelera sin necesidad de conocimientos técnicos
Desde kits de phishing hasta paquetes completos de malware e infostealers se ofrecen como servicios listos para usar.

4. Exploitación de infostealers y droppers a gran escala
Operaciones como Endgame y Magnus desactivaron plataformas masivas como Lumma, RedLine, META, y botnets como IcedID o Trickbot.

5. Brokers de acceso inicial (IAB) diversifican su oferta
Comercializan credenciales de acceso, shells web y servicios avanzados, incrementando el mercado de acceso inicial a redes comprometidas .

6. Herramientas cifradas y comunicaciones E2EE eluden la detección policial
Las apps con cifrado extremo-a-extremo facilitan transacciones delictivas, complicando la investigación y trazabilidad.

7. 'ClickFix': nueva táctica de ingeniería social con falsos mensajes del sistema
Los atacantes usan alertas falsas o captchas engañosos para inducir a los usuarios a ejecutar malware voluntariamente.

8. Amenazas desde el interior: insiders y suplantación de identidad
Empleados o perfiles falsos dentro de organizaciones son flecos críticos para filtrar información o instalar puertas traseras .

9. Recomendaciones clave de la IOCTA 2025
Entre ellas: acceso legal a datos cifrados, normas UE armonizadas sobre retención de datos, y campañas urgentes de alfabetización digital .