NEWS ADSI FLASH
www.adsi.pro

Índice

- Nuestros Patrocinadores.. 2
- Jornada sobre el nuevo Reglamento de Protección de Datos (GDPR) 3
- Security Forum 2018..... 4
- Día de la Seguridad Privada 2018 5
- Yihadismo y planeadoras (I) 6
- Bruselas excluye a las firmas de EEUU de los proyectos de defensa de la Unión..... 9
- XXXII Edición de los Trofeos de la Seguridad. 11
- Rusia 2018, el Mundial más vigilado: ¿Cómo será la seguridad?..... 14
- Un Plan Director de Seguridad garantizará el buen funcionamiento y la movilidad de los XVIII Juegos del Mediterráneo Tarragona 2018..... 15
- Tu Plan Director de Seguridad es esencial para abordar el RGPD..... 16
- ¿Que riesgos pueden suponer los asistentes inteligentes? 18
- Noticias..... 20
- Formación 21
- Promoción PortAventura Park 2018..... 21
- Legislación 21
- Revistas..... 22

Jornada sobre el nuevo Reglamento de Protección de Datos (GDPR)

28 de mayo de 2018

Exitosa jornada impartida por ADSI y PROSEGUR sobre el GDPR en el Auditorio AXA

Asociación de Directivos de Seguridad Integral
ADSI

PROSEGUR
Seguridad de confianza

General Data Protection Regulation

Nuestros Patrocinadores

Jornada sobre el nuevo Reglamento de Protección de Datos (GDPR)

Jornada impartida el pasado 28 de mayo de 2018 en el Auditorio AXA

ADSI junto con **PROSEGUR** celebraron el pasado lunes **28 de mayo en el Auditorio AXA de Barcelona** una jornada destinada al nuevo **Reglamento de Protección de Datos (GDPR)** de obligado cumplimiento desde el pasado 26 de mayo **y su impacto en Sistemas de Seguridad**.

La jornada fue todo un éxito tanto en el contenido como en la asistencia.

Durante la misma se pudieron resolver un sinfín de dudas sobre la aplicación del nuevo Reglamento sobre todo en aquello que concierne a los Sistemas de Seguridad.

La jornada se dividió en cuatro partes, la primera corrió a cargo de la abogada Dña. *Paloma Brú* de Pinset Masons que nos hizo un recorrido de los Servicios de Seguridad en el marco del GDPR, sin duda una intervención brillante que suscitó un sinfín de preguntas.

Prosiguió el Responsable Operativo de Grandes Cuenta de Prosegur, Don *Carlos Plasencia*, el cual repasó los servicios tecnológicos de seguridad dentro del marco del GDPR.

Don *Manel Pons*, Director de consultoría e integración de Prosegur nos adentró en el mundo de la Ciberseguridad y sus implicaciones con el GDPR.

Finalmente, un Foro-Debate con los tres ponentes suscitó numerosas preguntas que enriquecieron la jornada logrando que se convirtiera en todo un éxito.

Desde **ADSI** queremos agradecer la altísima capacitación de los ponentes y la magnífica asistencia a todos aquellos socios y amigos que tuvieron a bien acompañarnos.

Security Forum 2018

Junta Directiva

Con más de 7.000 asistentes esta edición de Security Forum ha vuelto a ser todo un éxito.

Celebrado en el CCIB de Barcelona en dos jornadas y con la presencia por primera vez de Hostelería y Contact Center.

El Global Day y el Ciber Day resultaron también todo un éxito y los premios se entregaron en la cena que contó con la presencia de Enric Millo, Delegado del Gobierno en Catalunya, acto en el que también se celebraron los 30 años de vida de la revista **Cuadernos de Seguridad**, desde aquí nuestra más que sincera enhorabuena por la inestimable contribución que hacen a la Seguridad.

Desde **ADSI**, que estuvo presente en el Stand nº 59, queremos agradecer a todos aquellos socios, patrocinadores y amigos que nos visitaron in-situ, como siempre resultó un enorme placer compartir un año más una edición del Security Forum con todos ellos.

La casualidad hizo que pudiésemos celebrar el cumpleaños de *Joan Roda*, amigo y miembro de Junta de **ADSI**, desde estas líneas deseamos poder repetir el próximo año tan entrañable momento.

Día de la Seguridad Privada 2018

Junta Directiva

El próximo **13 de Junio**, está previsto celebrar la **XV Edición del Día de la Seguridad Privada** en el Auditorio Procornellà, sito en calle Albert Einstein, 51 de Cornellà de Llobregat.

Este acto, organizado por la Delegación del Gobierno en Catalunya, Jefatura Superior de Policía de Catalunya, la 7ª Zona de la Guardia Civil y las Asociaciones del Sector de Seguridad Privada (ACAES, ADSI, AJSE, APROSER, ASES, Centros de Formación, Colegio de Detectives y APDPE), incluirá la distinción al personal de seguridad privada que durante el año pasado, han llevado a término acciones destacadas, en su actuación profesional o colaboración con la Seguridad Pública.

Está previsto que el acto esté presidido por el Excm. Delegado del Gobierno de Catalunya **Sr. Enric Millo**, junto con responsables policiales de Policía Nacional y Guardia Civil, así como de otros Cuerpos Policiales y otras Autoridades. El acto tiene como objetivo reafirmar la institución de un día al año en el que se celebre un encuentro de las Autoridades con las empresas de seguridad y el personal de seguridad privada, y dar la oportunidad para que la prensa se haga eco de las actuaciones meritorias del Personal de Seguridad, que muchas veces son ignoradas por la sociedad

El programa para los asistentes es el siguiente:

PROGRAMA

- **11:00 Recepción**
- **12.00 Acto de reconocimiento y entrega de galardones.**
- **13:00 Aperitivo**

Respecto al personal que recibe una mención, el programa es:

PROGRAMA

- **09:30 Recepción del personal mencionado y acreditaciones**
- **10:30 Distribución del personal dentro de la Sala**
- **12:00 Acto de reconocimiento y entrega de galardones**
- **13:00 Aperitivo**

Si alguno de los mencionados viene acompañado de algún familiar con minusvalía, rogamos nos lo hagan saber para habilitar su ubicación.

En relación a la uniformidad de los mencionados, será la siguiente:

Vigilante de Seguridad:

- **Uniformidad de verano**
- **Camisa de manga corta y sin corbata**
- **Placa**
- **Sin grilletes**
- **Sin defensa**
- **Sin gorra**

Detectives, Escoltas y Directivos de Seguridad: traje oscuro y se recomienda corbata.

Las Empresas que deseen asistir, tendrán que hacer llegar a ACAES antes del **4 de junio**, mediante correo electrónico, la relación nominal de asistentes, para poder hacer su reserva correspondiente.

Así mismo, será necesario transferir antes del día **4 de junio**, el importe de **35€** por persona (IVA incluido), al número de cuenta siguiente ***ES54-0081-0142-74-0001369140***. Para poder confirmar su reserva, es necesario que, una vez hecho el ingreso, y siempre antes del **4 de junio**, se haga llegar una copia del comprobante al correo electrónico *acaes@acaes.net*.

Yihadismo y planeadoras (I)

Fuente: MYS
Monitorización yihadismo y salafismo

Apenas a 13 Km de la frontera sur de Melilla, se encuentra la ciudad de Nador (Marruecos) a orillas de la Mar Chica, una laguna de 115 kilómetros cuadrados abierta al mar por una bocana de apenas 120 metros.

Con una configuración ideal para servir de refugio, hace años que alberga decenas de embarcaciones semirrígidas dotadas de tres a cinco motores de 300 caballos cada uno. Algunas de ellas aprovecharán las horas de oscuridad para surcar las olas del Estrecho a más de 120 kilómetros por hora cargadas con fardos de hachís que desembarcaran en las costas de la península. Son las conocidas popularmente como planeadoras.

Una embarcación estándar de unos 12 metros de eslora, transporta entre una y tres toneladas de hachís. Pongamos como ejemplo una carga intermedia de 1500 Kg, con un precio de salida en Marruecos de 600.000 euros, una vez desembarcados en España, su valor se multiplica por 20 pasando a ser 12 millones de euros.

Tres personas componen la tripulación: piloto, copiloto y encargado de motores, que reciben por cada viaje unos 27.000, 5.000 y 3.500 euros respectivamente.

La presión policial en la zona del Estrecho, ha provocado que las rutas se diversifiquen para llevar la droga más lejos. Para ello, sitúan embarcaciones nodriza repletas de garrafas de combustible en puntos estratégicos de avituallamiento, previamente establecidos para que las planeadoras reposten combustible. De esta manera, y en varias etapas han podido llegar a desembarcar los fardos de hachís en Ibiza, el delta del Ebro, Girona e incluso Marsella.

Esta actividad se está viendo alterada desde hace un par de años por tres factores que están multiplicando los niveles de riesgo y que con toda seguridad harán evolucionar la situación a escenarios de gran peligrosidad.

En primer lugar, la irrupción de bandas que haciéndose pasar por policías o simplemente a las bravas y empleando armas de fuego, están robando los alijos de droga a los narcotraficantes. Esto ha tenido como consecuencia que ahora unos y otros van fuertemente armados, y no solo con pistolas o revólveres, sino con subfusiles y fusiles de asalto.

Por otro lado hay que tener en cuenta la aparición en ambas orillas del Estrecho, de elementos pertenecientes a los cárteles sudamericanos de la cocaína, que pretenden aprovechar en beneficio propio las infraestructuras y rutas del tráfico de hachís.

Y por último, la radicalización que se está produciendo en algunos de los musulmanes dedicados al narcotráfico, al tener unos vínculos cada vez más fuertes con el salafismo, llegando en algunos casos a poder considerarlos como de ideología yihadista.

Descripción

El presente trabajo se ha llevado a cabo durante 5 meses (enero-mayo 2018) en los cuales se ha monitorizado la presencia en redes sociales de 30 individuos vinculados entre sí, pero con diferentes niveles de radicalización y desempeñando diversas funciones dentro del narcotráfico.

La falta de información sobre identidades y en algunos aspectos operativos, es necesaria para no perjudicar la función de los investigadores a quienes MYS ha facilitado todos los datos.

Los individuos se denominaran como “sujeto” del 1 al 30. Todos ellos son hombres, detectándose la presencia minoritaria de mujeres en funciones de atención del hogar y cuidado de los hijos, evitando incluso que se vean sus rostros en las fotografías.

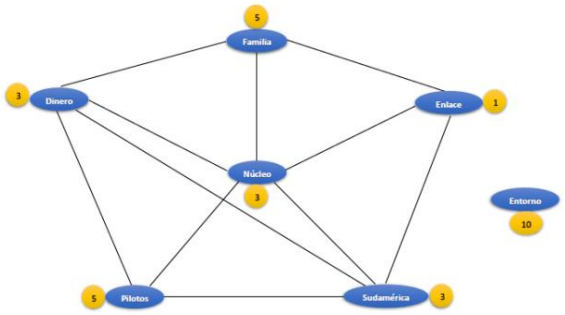
Esta es la primera de varias partes en que se dividirá el análisis. Aquí se tratan los aspectos técnicos sobre la composición de la estructura organizativa, rol de sus

miembros, ubicación, niveles de radicalización y vínculos entre ellos.

En próximas entregas se desarrollarán los aspectos humanos y situaciones personales de muchos de los individuos, estudiando su ideología, comportamiento y niveles de radicalización.

Organización y estructura

En función del rol que desempeñan los 30 sujetos, pueden dividirse en los 7 apartados siguientes:

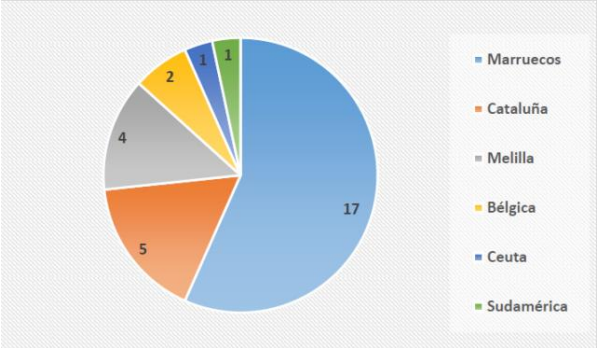


- Núcleo: compuesto por 3 individuos que dominan las comunicaciones y están ubicados en Cataluña. Son los únicos que están conectados e interactúan con todos los demás grupos.
- Dinero: se trata de 3 personas con un nivel de vida muy por encima del resto. Hacen ostentación de lujosas casas, coches de alta gama, ropa de marca y toda clase de complementos de los mejores fabricantes. Además publican numerosas fotografías con enormes fajos de dinero. Para blanquear el dinero del narcotráfico crean negocios como restaurantes y agencias de viaje. Están ubicados en Melilla y tienen relación con todos los demás grupos excepto con el enlace.

- Familia: compuesta por un grupo básico de 5 individuos que se ramifica a otros miembros de la familia de menor relevancia. Estos 5 perfiles se relacionan con el núcleo, dinero y enlace.
- Enlace: un curioso elemento que desde Cataluña tiene contacto con los grupos de núcleo, familia y Sudamérica, además de vínculos con un detenido por yihadismo en Cataluña en 2017. Se desenvuelve y contacta con todos pero manteniendo un trabajo normal y vida anodina.
- Pilotos: este grupo de 5 personas engloba tanto pilotos como copilotos de planeadoras. Tienen relación con los grupos de núcleo, dinero y Sudamérica.
- Sudamérica: 3 sujetos, de los cuales 2 se encuentran en el norte de Marruecos y uno en Sudamérica. Tienen relaciones con presuntos miembros de los cárteles sudamericanos de la cocaína. Utilizan diferentes formas encubiertas para comunicarse.
- Entorno: el resto de las 10 personas que pululan alrededor de los perfiles de los grupos ya comentados. Realizan funciones secundarias, estando radicalizadas algunas de estas personas.

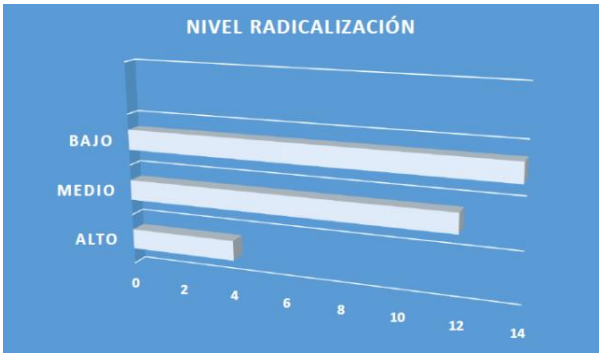
Ubicación de los sujetos

Tal como se ha mencionado en el apartado anterior, el núcleo central se encuentra en Cataluña. El grupo del dinero en Melilla. La familia y los pilotos están en Marruecos. El enlace en Cataluña. Del grupo que se relaciona con Sudamérica dos están en Marruecos y uno en Sudamérica. Y por último los 10 del entorno son: 5 de Marruecos, 2 de Bélgica y uno de Ceuta, Melilla y Cataluña respectivamente.



Niveles de radicalización

Teniendo en cuenta diferentes factores como ideología, contenidos en redes sociales, vínculos e interacciónes con detenidos por yihadismo, se han especificado tres niveles de radicalización denominados bajo, medio y alto en sentido ascendente de intensidad.



Obteniendo un resultado de 14 sujetos con una baja radicalización, 12 en nivel medio y 4 altamente radicalizados. De éstos últimos, 3 están en Cataluña, perteneciendo 2 al núcleo y el enlace, y el otro de alta radicalización pertenece al grupo de la familia en Marruecos.

Vínculos con yihadista detenido

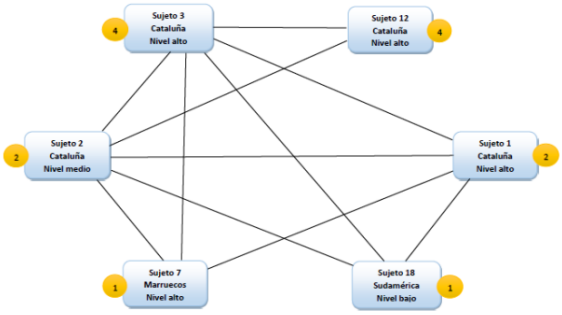
Seis de las personas monitorizadas tienen vínculos con un yihadista detenido en Cataluña durante 2017. Concretamente 2 de los sujetos (núcleo y enlace) tienen 4 vínculos, otros 2 individuos (núcleo) tienen 2 vínculos y los 2 últimos (familia y Sudamérica) tienen un vínculo.

Liderazgo

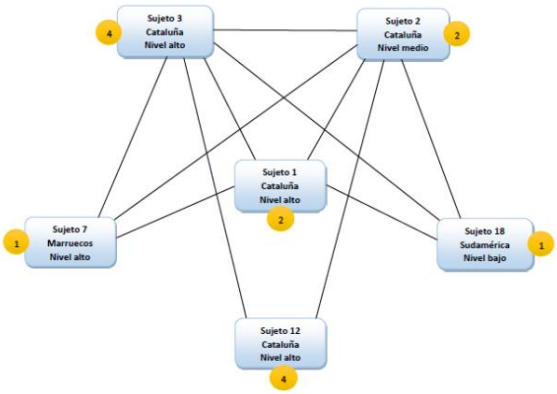
Tras estudiar los 6 sujetos que tienen vínculos con el yihadista detenido en 2017, se ha podido determinar la relevancia de cada uno dentro del grupo.

Cruzando estos resultados con las interacciones entre ellos, se obtienen dos gráficos que permiten visualizar la relevancia de cada individuo.

En croquis inferior se analiza la intensidad de las relaciones con el yihadista detenido, pudiendo observar junto a los 6 perfiles un círculo naranja donde consta la cantidad de vínculos con el detenido. Clasificados de mayor a menor, los cuatro primeros sujetos serían: 3, 12, 2 y 1.

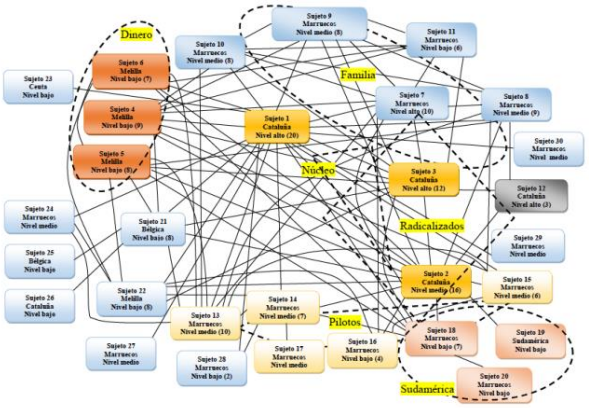


El croquis inferior representa los vínculos de interacción entre los propios sujetos al nivel del narcotráfico, obteniendo como resultados más altos los sujetos: 3, 2 y 1.



Del resultado obtenido, podemos considerar que los sujetos denominados 1, 2 y 3 son los que tienen más relevancia dentro del grupo.

Para finalizar el análisis, se muestra un gráfico de los 30 perfiles con los vínculos entre sí, agrupados en los diferentes apartados según el rol de cada uno. Dentro de cada recuadro se incluye la información de: número de sujeto, lugar de ubicación, y en la línea inferior el nivel de radicalización, acompañado entre paréntesis de la cantidad de vínculos que tiene.



Bruselas excluye a las firmas de EEUU de los proyectos de defensa de la Unión

Fuente: El País

Lucía Abellán – Claudi Pérez

La Comisión solo financiará planes en los que participen al menos tres países miembros

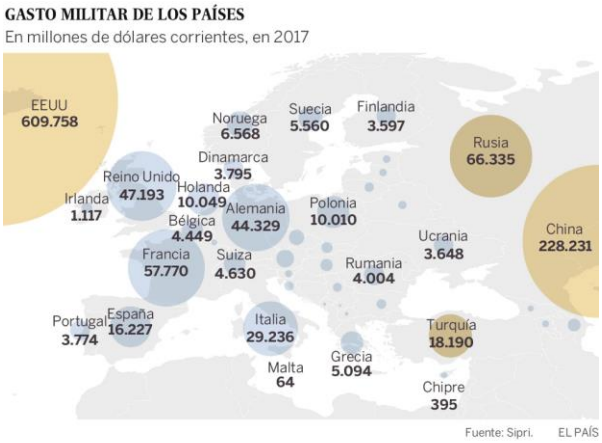
La autonomía estratégica de Europa en defensa constituye una aspiración que irrita a EE UU. Pero la creciente desconfianza europea hacia su teórico aliado acelera los planes para despegarse poco a poco de Washington. La Comisión Europea presenta esta semana los tres instrumentos que pretenden mejorar el músculo militar de la UE al margen de la OTAN. El principal es un fondo de 13.000 millones de euros para desarrollar equipos que excluye a empresas extranjeras (salvo excepciones) con el fin de reforzar la industria europea. La UE se colocará así entre los cuatro primeros inversores del continente en tecnología de defensa.

La cooperación militar pesa cada vez más en la agenda europea. Superadas las reticencias históricas —casi nadie osaba apoyar la inversión militar en un club que nació como garantía de paz en el continente—, Bruselas aprovecha la convulsa situación exterior para apuntalar la defensa común. "Europa afronta nuevas amenazas que no conocen fronteras y ningún país europeo las puede afrontar por separado. En un entorno internacional cambiante, Europa necesita reforzar su autonomía estratégica", defiende el Ejecutivo comunitario en un borrador al que ha tenido acceso EL PAÍS.

La defensa del bloque comunitario depende en estos momentos bastante de Estados Unidos, que presta asistencia —y vende equipos— a sus aliados europeos. La Administración de Donald Trump observa con enorme recelo cualquier intento europeo de potenciar la industria armamentística comunitaria. Porque aunque Trump no se ha cansado de repetir que la UE tiene que gastar más en el ámbito militar y en su propia defensa, su mensaje daba por sentado que ese dinero acabaría en manos de empresas estadounidenses, líderes en estos proyectos. Justo lo contrario de lo que persiguen las herramientas que ha ideado Bruselas, aunque está por ver que lo logren.

El Ejecutivo comunitario presentará este miércoles el nuevo Fondo Europeo de Defensa, dotado con 13.000 millones de euros "para defender y proteger a los europeos", según el documento consultado. Esa partida, que está prevista para el periodo presupuestario 2021-2027, pretende impulsar la inversión en equipamiento militar, con reglas claras para evitar acabar financiando a empresas controladas por países terceros, entre ellos Estados Unidos.

Aun así, Bruselas abre la posibilidad a algunas exenciones de la norma. Se podrá financiar a filiales europeas de empresas radicadas en el exterior a condición de que no haya transferencias de información clasificada (algo fundamental en un ámbito estratégico como la defensa). El Ejecutivo comunitario ha incluido esta salvedad por la insistencia del Consejo de la Unión, que representa a los Estados miembros y que temía que muchos proyectos industriales pudieran quedar fuera del paraguas financiero común por desarrollarse en colaboración con firmas extranjeras.



Elevar la inversión

Europa ya puso en marcha el año pasado una primera versión de ese fondo. Pero la cantidad habilitada para los próximos presupuestos supera con creces los apenas 600 millones de euros fijados entre 2018 y 2020 en el proyecto piloto. Los 13.000 millones programados para las próximas cuentas europeas (lo que supone unos 1.800 millones anuales) se dividirán en dos apartados: 4.100 millones para proyectos de investigación militar y 8.900 millones adicionales para desarrollar capacidades de defensa (tanques, drones, programas de ciberseguridad…) en proyectos en los que participen al menos tres Estados miembros. El objetivo es fomentar la cooperación.

Las condiciones impuestas por Bruselas son exigentes. Solo se financiarán iniciativas que se ajusten a las prioridades de la UE, con participación de pequeñas y medianas empresas. La Comisión aportará el 20% del desarrollo y el resto lo

abonarán los Estados interesados en poner en marcha esos equipos (y en adquirirlos posteriormente).

La cofinanciación comunitaria puede subir hasta el 30% del coste del proyecto si la iniciativa pertenece al núcleo duro de la defensa que conformaron el año pasado 25 Estados miembros para avanzar más en su integración militar (PESCO, por sus siglas en inglés). "El 5% de los fondos se destinarán a innovación, a tecnologías disruptivas", asegura el documento. Es decir, a tecnologías que cambien radicalmente el mercado, como los drones o el encriptado de información.

Los expertos muestran cautelas respecto al futuro de la política europea de defensa, una de las pocas que suscita acuerdos mayoritarios. "No sé si ya tenemos consenso, pero Angela Merkel ha dado un paso adelante en su respuesta a Emmanuel Macron y el hecho de que la Administración de Trump no proteja, sino que más bien desestabilice y humille a la UE, funciona como pegamento", reflexiona Sébastien Maillard, del Instituto Delors. Maillard se refiere al respaldo que ha otorgado la canciller alemana a la fuerza de intervención rápida para situaciones de crisis que ha propuesto el presidente francés.

Más escéptico, Charles Wyplosz, de la institución especializada en relaciones internacionales Graduate Institute, concluye: "El único ejército eficaz es el francés. El otro es el británico, pero se va de la UE. El Ejército alemán no existe. Y lo militar es un medio, no un fin. No se ve cuál sería el fin común".

MÁS DE 10.000 MILLONES PARA LA GUERRA Y LA PAZ

Junto al fondo para la industria europea de defensa, Bruselas activa también el llamado Instrumento Europeo de Paz, dotado con 10.500 millones de euros para el periodo 2021-2027. Pese a su nombre, esta herramienta pretende financiar actividades militares desarrolladas en países terceros. El dinero sería ajeno al presupuesto comunitario (lo aportarían directamente los Estados) y se destinaría a apoyar a dichos terceros países con infraestructuras, equipos y asistencia técnica. Un ejemplo de este tipo de operaciones sería la financiación de la UE al llamado G5, una fuerza de 5.000 soldados africanos que trata de estabilizar el Sahel, región lastrada por el yihadismo y las mafias. En lugar de implicarse en contiendas externas, Europa ofrece así recursos para que las fuerzas locales sofoquen los conflictos de sus territorios.

El tercer proyecto se refiere a la movilidad militar. Bruselas reservará 6.500 millones del mecanismo denominado Conectar Europa (el gran capítulo de inversión en infraestructuras del presupuesto comunitario) para garantizar el transporte de vehículos militares y de soldados a lo largo de la Unión. Uno de los objetivos que tiene este plan es que carreteras y puentes puedan soportar el peso de esos peculiares desplazamientos (por ejemplo, de tanques) en caso de que fuese necesario moverlos por el territorio comunitario. Ese gesto —dedicar dinero europeo a adecentar infraestructuras civiles por motivos militares— hubiese sido impensable hace apenas unos años.

XXXII Edición de los Trofeos de la Seguridad

Fuente: Seguritecnia

¡Anímate a participar en el certamen más prestigioso de la seguridad! Un evento en el que se reconoce públicamente a las empresas y profesionales del sector más destacados del año. El plazo de admisión de candidaturas finaliza el próximo 30 de julio.

La revista Seguritecnia abre el proceso de recepción de candidaturas para la XXXII Edición del Certamen Internacional de los Trofeos de la Seguridad. Un evento en el que se reconoce públicamente a las empresas y profesionales del sector más destacados del año y al que asisten importantes representantes de la Administración, de las Fuerzas y Cuerpos de Seguridad y numerosos profesionales del sector que quieren estar presentes en el acontecimiento. Javier Borredá, presidente de Editorial Borrmart, resaltó en la pasada edición del certamen que: "los trofeos representan un ejemplo de compromiso, profesionalidad y servicio a la Seguridad". Los expedientes quedarán con carácter confidencial en poder de la revista. El plazo de admisión de inscripción permanecerá abierto hasta el próximo 30 de julio.

La revista Seguritecnia publicará el fallo del jurado y los premiados recibirán los trofeos en el "Almuerzo de la Seguridad" que se celebrará en el último trimestre del año. Estos trofeos, que son honoríficos, se materializarán en una placa artística que, a modo de diploma, los perpetúa.

Los trofeos serán otorgados por el jurado, constituido por el Pleno del Consejo Técnico Asesor de Seguritecnia, a las personas o entidades acreedores a ellos, desde la anterior edición del certamen, en las siguientes modalidades:

Trofeos

- T1.- TROFEO AL MEJOR PRODUCTO DE SEGURIDAD comercializado en España y/o en la Unión Europea.
- T2.- TROFEO AL MEJOR SISTEMA DE SEGURIDAD instalado y operativo en España y/o en la Unión Europea.
- T3.- TROFEO A LA ACTIVIDAD INVESTIGADORA (I + D) en materia de seguridad en España y/o en la Unión Europea.
- T4.- TROFEO AL MÉRITO EN LA TRAYECTORIA PROFESIONAL EN SEGURIDAD PRIVADA, al profesional de la seguridad privada, empresa prestataria o usuaria que, habiendo estado en activo durante más de 15 años, se haya destacado por su trayectoria profesional o empresarial, reconocimiento del sector de la Seguridad Privada o aportación al mismo.
- T5.- TROFEO AL DIRECTIVO USUARIO DE SEGURIDAD PRIVADA, al directivo de entidad usuaria de seguridad que haya destacado por su trayectoria profesional y aportación al sector de la Seguridad Privada.
- T6.- TROFEO AL MÉRITO EN EL SERVICIO EN LA SEGURIDAD PRIVADA, al personal de Seguridad Privada regulado en la Ley 5/2014 (es decir: vigilante de seguridad, vigilante de explosivos, escolta privado, guarda rural, guarda de caza, guardapesca marítimo, jefe de seguridad, director de seguridad y detective privado), que haya tenido un comportamiento altruista y destacado en el cumplimiento de sus funciones legales, por encima del cumplimiento exigible de su deber.
- T7.- TROFEO AL MÉRITO EN EL SERVICIO EN LA SEGURIDAD PÚBLICA, a aquellos componentes o Unidades de las Fuerzas y Cuerpos de Seguridad (estatales, autonómicas o locales) que se hayan distinguido por un comportamiento destacado, por encima del cumplimiento exigible de su deber, en la protección de los ciudadanos, en defensa de la Ley o de la seguridad pública.
- T8.- TROFEO AL MÉRITO EN LA PROTECCIÓN CIVIL, a los componentes de los servicios de prevención y extinción de incendios, salvamento, rescate, protección civil, etc., que se hayan distinguido por un comportamiento destacado, por encima del cumplimiento exigible de su deber, en situaciones de riesgo, ayuda humanitaria o en acciones preventivas en la materia.
- T9.- TROFEO A LA FORMACIÓN EN SEGURIDAD, a la persona, entidad o empresa que más haya destacado por la calidad de la enseñanza, innovación en sistemas pedagógicos, medios y métodos docentes.
- TE.- TROFEO EXTRAORDINARIO DEL JURADO, a la persona, entidad o colectivo que haya destacado extraordinariamente por sus acciones meritorias o su servicio prolongado en provecho de la seguridad, en el ámbito nacional o internacional.

Jurado

El Jurado del Certamen se constituye en el seno del Consejo Técnico Asesor de Seguritecnia, convocado y reunido a tal efecto según su normativa específica, comunicada a sus miembros bajo la Presidencia de su titular, quien, previo análisis de los dictámenes no vinculantes de las Comisiones de Estudio designadas por el mismo, decidirá la concesión de los Trofeos de la correspondiente edición anual.

El Jurado podrá conceder más de un premio en alguna de las especialidades cuando lo considere preciso, por la alta calidad e igualdad de algunas de las propuestas presentadas.

También puede declarar desierto alguno o algunos de los Trofeos si, a su juicio, no se reúnen los méritos suficientes. Sus decisiones son inapelables.

Requisitos de presentación de las propuestas

- Idioma: la documentación técnica y descripción del producto/actividad serán en castellano.
- Las propuestas han de presentarse necesariamente en soporte informático e incorporarán también una copia en papel.Se tienen que remitir a la redacción de la revista Seguritecnia (C/ Don Ramón de la Cruz 68, 6º. 28001. Madrid) mediante correo postal o a través del correo electrónico: trofeos.seguritecnia@borrmart.es, siendo obligatoria la cumplimentación del formulario dependiendo del trofeo al que se presente (los puedes rellenar online al final de la noticia).
- Se valorará positivamente toda presentación sintetizada y gráfica que facilite su análisis por la Comisión.
- Las candidaturas han de contener los datos filiación/identificación completa del proponente y del candidato.
- No podrá presentarse una misma candidatura a las categorías T1 y T2.
- Las candidaturas sólo podrán presentarse por parte de:

Categorías T1, T2, T3, T6, T7, T8 y T9: cualquier persona o entidad conocedora de los méritos de la candidatura, así como cualquiera de los miembros del Jurado.

Categorías T4, T5 y TE: cualquiera de los integrantes del Jurado, que no podrán presentarse a sí mismos, ni a las entidades a las que representen, ni aquellas otras en las que tengan intereses de cualquier índole.

Configuración de las Comisiones de Estudio (T1, T2, T3, T7, T8 y T9)

Las Comisiones de Estudio estarán constituidas por los integrantes del Jurado (con posibilidad de sustitución regulada en las normas del Jurado), acordadas en sesión plenaria con tal finalidad. Dichas Comisiones evaluarán las diversas propuestas presentadas, analizando si cumplen los requisitos exigibles a cada modalidad, y definirán de entre ellas las que se someten, como finalistas, a la votación del Jurado.

Con carácter general, y salvo otro acuerdo del Pleno, se nombrarán dos Comisiones:

PRIMERA COMISIÓN:
Dictaminará las modalidades T1, T2 y T3. Evaluará los siguientes aspectos:

-Requisitos de carácter técnico:

- Presencia del producto en el mercado.
- Presentación de certificaciones de acuerdo con la normativa vigente, si existen.
- Presentación de homologaciones de acuerdo con la normativa vigente, si existen.

-Requisitos de disponibilidad para análisis presencial por la Comisión que ha de garantizar el concurrente:

- Disponibilidad del aparato/equipo/sistema, para estudio directo por la Comisión.
- Disponibilidad de realización de ensayos, si lo considerase pertinente la Comisión.

SEGUNDA COMISIÓN:
Dictaminará los Trofeos T7, T8 y T9. Evaluará los siguientes aspectos:

- Requisitos que comprenden valores humanos, en general y profesionales, en particular.
- Memoria personalizada de los hechos, historiales profesionales u otros antecedentes que ayuden al mejor conocimiento de los méritos por parte de la Comisión.

PROCEDIMIENTO ESPECIAL PARA LAS MODALIDADES TE, T4, T5 y T6

El Trofeo Extraordinario y las modalidades T4, T5 y T6 se debatirán y acordarán por el Pleno directamente, sin participación de Comisión de Estudio alguna.

Estas candidaturas deben ser propuestas por escrito dirigido telemáticamente a la Secretaría del Jurado, pudiendo unir al escrito de la propuesta cuanta documentación se considere oportuna para acreditar los méritos del candidato. La propuesta deberá ser efectuada por uno o varios miembros

del propio Jurado, siempre que no se presenten a sí mismos, ni a las entidades a las que representen, ni aquellas otras en las que tengan intereses de cualquier índole.

Con carácter general, no se admitirán propuestas en la misma sesión del Jurado, salvo que lo haga el Presidente del mismo a la vista de las candidaturas presentadas o que el Jurado decida ampliar el plazo.

Gastos derivados del estudio de las propuestas

Los posibles gastos derivados de las visitas, análisis, ensayos, contrastes, etc., que requiera la respectiva Comisión de Estudio para emitir su dictamen –cuyos resultados quedarán en poder de la candidatura al premio– serán sufragados por el candidato correspondiente, una vez se le comunique su candidatura y la acepte.

Entrega de candidaturas

Las candidaturas propuestas (excepto las de los Trofeos T4, T5, T6 y Extraordinario, que se pueden formular y entregar en el propio seno del Jurado), se remitirán mediante correo postal a la Secretaría del Jurado, en la revista SEGURITECNIA (C/ Don Ramón de la Cruz 68, 6º. 28001. Madrid).

También se enviará toda la documentación al correo electrónico trofeos.seguritecnia@borrmart.es

El plazo máximo de presentación de candidaturas finaliza el 30 de julio de cada año, para los premios correspondientes a dicho ejercicio, salvo lo que resuelva el propio Jurado dentro de sus deliberaciones.

Los expedientes quedarán tratados con la necesaria confidencialidad, estarán en poder de la revista y no se notificará resolución alguna sobre los mismos, salvo a las candidaturas ganadoras.

Entrega de los premios

La revista Seguritecnia publicará el fallo del jurado, y los premiados recibirán sus Trofeos en el "ALMUERZO DE LA SEGURIDAD" que, a esos efectos, se celebrará en el último trimestre del año.

Estos Trofeos, que son honoríficos, se materializarán en una placa artística que los perpetúa. A petición del interesado se expedirá la credencial correspondiente.

Trofeo Ramón Borredá

FUNDACIÓN BORREDÁ
al servicio de la seguridad

El Trofeo "Ramón Borredá" se crea para distinguir a la persona que haya demostrado mayor entusiasmo y excepcional esfuerzo por el desarrollo positivo de la Seguridad, pública o privada, en un marco ético.

El Trofeo "RAMÓN BORREDÁ" se constituye como el primero y más importante del Certamen Internacional "Trofeos de la Seguridad".

Tendrá periodicidad anual y se otorga a la memoria del fundador de Seguritecnia, Don Ramón Borredá García como estímulo para los profesionales de la seguridad en atención a méritos y valores singulares. Este Trofeo no podrá ser compartido.

Se concederá por acuerdo del Patronato de la Fundación Borredá para la Seguridad constituido en Jurado y se entregará en el mismo acto que el Certamen Internacional "Trofeos de la Seguridad".

Más información en el siguiente enlace

Rusia 2018, el Mundial más vigilado: ¿Cómo será la seguridad?

Fuente: La Vanguardia
DPA, Moscú

Tras los violentos enfrentamientos entre "hooligans" rusos e ingleses en la Eurocopa de Francia 2016, Rusia ha estado tomando estrictas medidas para combatir la violencia ultra en los preparativos del Mundial de fútbol.

A más de 400 hinchas violentos conocidos se les ha prohibido acudir a los partidos, según una lista publicada por el Ministerio del Interior. Además, todo aquel que haya comprado una entrada debe adquirir también una tarjeta de identificación personal para ingresar a los estadios, conocida como "Fan ID". La entrada al estadio le puede ser impedida si surge algún tipo de sospecha.

Unos de los líderes de los ultras rusos dijo que a unas mil personas que habían comprado entradas se les impidió ingresar a los partidos en la Copa Confederaciones del año pasado, que Rusia albergó como un ensayo del Mundial.

"Mi identificación y las de unas mil personas fueron invalidadas, incluso aunque ningún tribunal haya dictaminado nada al respecto", explicó a dpa Alexander Shprygin, que lidera la Unión de Hinchas Rusos.

"Ahora justo antes del Mundial, la policía está realizando un trabajo especial de cara a los hinchas. No pasan por alto ni una violación a una norma en un estadio", señaló Shprygin.

"Creo que no habrá ninguna pelea porque la policía intervendrá inmediatamente", añadió. "La Copa del Mundo en Rusia será una de las más seguras en la historia del torneo".

Tras los enfrentamientos en Francia, Rusia endureció sus leyes contra los hinchas violentos. Incluso los simpatizantes que causen el menor disturbio durante un partido pueden ir a parar a la cárcel.

En un gesto de resarcimiento, los hinchas del Manchester United fueron recibidos muy cordialmente en febrero de 2017 en la ciudad de Rostov del Don, en el sur de Rusia. Los acomodadores de aquel partido de la Liga Europa les ofrecieron incluso mantas.

Fue el primero de una serie de eventos en los que se recibió con amabilidad a los simpatizantes, con el fin de presentar a Rusia como un anfitrión cordial.

Rusia asignó 11.000 millones de dólares a los preparativos del Mundial. El torneo es promocionado como una oportunidad de impulsar el turismo en los años venideros, ya que serán miles las personas que visitarán el país en las próximas semanas.

La mayor cantidad de solicitudes de tarjetas de identificación provino de Estados Unidos, seguido de México y China, según dio a conocer el Ministerio de Comunicación ruso a mediados de abril.

Estas tarjetas de identificación, conocidas como "Fan ID", también permitirán a sus portadores viajar a Rusia durante el torneo sin visa, según comunicó la FIFA en su página web. Indicaciones en inglés en los estadios y en la infraestructura de transporte, junto con un equipo multilingüe, apuntan a ayudar a los numerosos visitantes a no perderse.

Andrei Chernenko, funcionario del Ministerio de Comunicación, se mostró encantado con que tantos estadounidenses acudan al torneo a pesar de las tensiones entre los Gobiernos de Estados Unidos y Rusia.

El presidente de Estados Unidos, Donald Trump, escribió recientemente en Twitter que la relación entre Estados Unidos y Rusia está en uno de sus peores momentos.

"La situación, que ha sido inflada por los medios masivos de comunicación, no tiene ningún impacto", aseguró Chernenko en comentarios difundidos por la agencia rusa TASS. "Las solicitudes de estadounidenses siguen llegando y la tendencia es positiva".

Rusia también tomó medidas severas contra el aumento de precios en los hoteles en vísperas del Mundial. Unos 600 hoteles fueron multados por unos 100.000 dólares por inflar los precios, según la agencia rusa de protección del consumidor, Rospotrebnadzor.

El Ministerio de Situaciones de Emergencia tendrá unos 40.000 trabajadores especializados en los partidos para garantizar la seguridad. El Ministerio de Comunicación señaló que incluso custodiará la infraestructura tecnológica para evitar cualquier problema con Internet.

Un Plan Director de Seguridad garantizará el buen funcionamiento y la movilidad de los XVIII Juegos del Mediterráneo Tarragona 2018

Fuente: Tarragona 2018

La Policía de la Generalitat-Mossos d'Esquadra, juntamente con el Ayuntamiento de Tarragona y el Comité Organizador del evento, han impulsado un Plan Director de Seguridad para abordar de manera integral la seguridad de las competiciones, los participantes, visitantes y residentes durante la celebración de los Juegos Mediterráneos.

La seguridad de los Juegos Mediterráneos Tarragona 2018 ha abordado desde el trabajo en red y transversal de la multiplicidad de operadores que se coordinarán durante los días que durará el evento para poder dar respuesta rápida y eficaz a posibles incidencias que se puedan generar a lo largo de la celebración. Además, la situación actual de nivel 4 sobre 5 de alarma terrorista ha sido uno de los puntos clave en la elaboración de este Plan Director de Seguridad.

Por parte de la PG-ME participarán todas las especialidades, desde la Unidad Canina, la Unidad de subsuelo, el TEDAX, la Unidad Aérea hasta el Grupo Especial de Intervención formarán parte del dispositivo policial que tiene que garantizar la seguridad de esta cita deportiva de carácter internacional. El dispositivo de seguridad incorporará drones al sistema de vigilancia y control previstos en este evento que transmitirán datos en directo en centros de mando.

Por su parte, la Guardia Urbana de Tarragona ha establecido un dispositivo que desplegará prácticamente a todos los efectivos durante la celebración de los Juegos, para dar cobertura, en coordinación con los otros operadores de seguridad, la seguridad de este evento y la de los actos paralelos previstos, así como los requerimientos de movilidad en la ciudad.

Dispositivos preventivos de seguridad ciudadana

Los Mossos, junto con la Guardia Urbana de Tarragona y con las Policías Locales de los municipios donde se llevarán a cabo las correspondientes competiciones deportivas, materializarán un plan de seguridad en las sedes de las competiciones. En este ámbito, trabajarán coordinadamente con efectivos de las empresas de seguridad privada que participarán en la seguridad de las instalaciones, accesos y alojamientos.

Movilidad ordenada

En cuanto a la movilidad, la División de Transportes (DTR) de la Comisaría General de Movilidad (CGMO) y el Área Regional de Tráfico (ART) de Tarragona de la División de Tráfico (DT) de la Policía de la Generalidad Mossos, aplicarán un plan de movilidad y seguridad vial en el territorio del evento.

Se ha trabajado el aspecto de la movilidad desde tres vertientes: la formación en conducción segura de los voluntarios de los JMT, la formación de las Policías Locales / Guardia Urbana que forman parte del PDS de los Juegos en materia de transporte de viajeros, y el diseño del correspondiente Plan de Movilidad.

El Plan de Movilidad contempla 11 rutas seguras para el traslado de deportistas y de otros miembros de la organización, estas rutas parten todas de la villa mediterránea con destino al resto de sedes descentralizadas y centros hospitalarios de la zona.

Se incrementarán los efectivos en zonas de especial influencia como son las llegadas y salidas de pasajeros en el aeropuerto de Barcelona y Reus, en las estaciones de ferrocarriles, así como, en las estaciones de autobuses.

En relación a las restricciones de tráfico originadas en motivo de la celebración de alguna de las competiciones deportivas, se tiene previsto afectaciones los días 27 y 30 de junio en vías interurbanas y urbanas con motivo de las pruebas de ciclismo contrarreloj y ciclismo en ruta.

Información y consejos de seguridad antes y durante los JMT 2018

La Policía de la Generalidad de Cataluña – Mossos llevará a cabo una campaña informativa para hacer llegar a los participantes y espectadores información útil y consejos de seguridad.

El PDS incluye la comunicación con el sector hotelero del campo de Tarragona y Barcelona para orientar e informar sobre medidas de autoprotección dirigidas a los visitantes y a las delegaciones deportivas.

Los Mossos y la Guardia Urbana de Tarragona a través de sus perfiles en redes sociales, y en colaboración con el Comité Organizador, pondrá a disposición de los ciudadanos información de seguridad y consejos para evitar ser víctimas de cualquier ilícito penal.

Tu Plan Director de Seguridad es esencial para abordar el RGPD

Instituto Nacional de Ciberseguridad

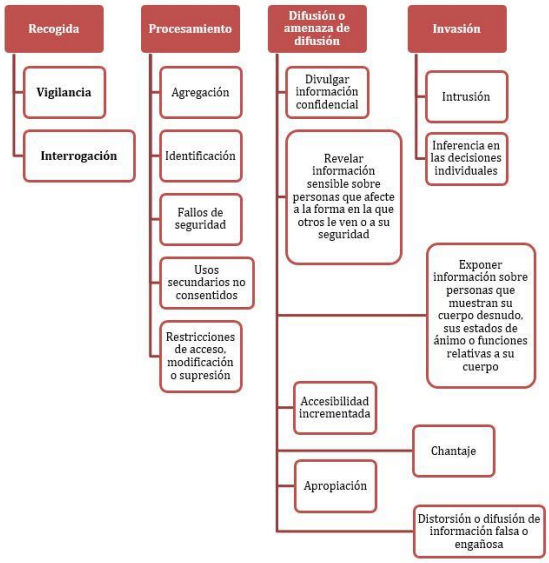
Con la obligación de cumplir el RGPD a partir del próximo 25 de mayo y el desarrollo del nuevo reglamento de ePrivacy, a los que se añaden las recientes noticias de brechas de datos personales, los debates sobre privacidad están de moda. La digitalización de muchos servicios públicos, del comercio y de la vida social, nos plantean dudas sobre si aún nos queda algún resquicio de intimidad. La red sabe dónde estamos, qué intereses tenemos, cuál es nuestro estado de salud, qué compramos, quienes son nuestros amigos,…

Dejando a un lado a los organismos públicos a los que se les supone un esmero en el cuidado de nuestra privacidad, el resto de organizaciones, pymes y autónomos se ven ahora también ante la tesitura de esforzarse un poco más en este aspecto con la nueva normativa.

Pero, ¿qué es la privacidad?, y… ¿cómo nos afecta?

Los datos personales son tanto aquellos que nos identifican (nombre, apellidos, DNI) como los que tienen que ver con nuestra situación laboral, financiera o de salud. También se incluyen ahora los datos biométricos y los biológicos. Es decir, cualquier información con la que se nos identifique o se nos pueda identificar. Algunos como los relativos a salud, ideología, religión, origen racial, vida sexual y comisión de infracciones penales y administrativas, están especialmente protegidos en el RGPD.

Existen cuatro grupos de actividades que pueden afectar a la privacidad



1. **Recogida:** actividades mediante las cuales se obtiene, sin permiso o con abuso de autoridad, información de carácter personal.
2. **Procesamiento:** actividades que se realizan procesando de alguna forma la información personal durante su almacenamiento o manipulación una vez recogida.
3. **Difusión o amenaza de difusión:** actividades que implican una revelación de, o la amenaza de revelar, información personal.
4. **Invasión:** actividades que irrumpen en la vida privada de las personas.

¿Qué puedo hacer para proteger la privacidad de mis clientes, empleados y proveedores?

Así visto, parece razonable proteger los datos personales de nuestros clientes, empleados o proveedores. Velar por la privacidad es algo que puede favorecer la confianza en nuestro negocio.

En la empresa los **riesgos para la privacidad**, los que debemos gestionar, derivan fundamentalmente de:

- No ser transparentes al informar sobre el tratamiento de los datos y no pedir el consentimiento adecuado.
- Tomar más datos de los necesarios o tomar datos cuya recogida no es legítima, para los que no estamos autorizados.
- No permitir o impedir a los propietarios de los datos ejercer sus derechos.
- Procesar los datos personales de forma descuidada o sin tener en cuenta los efectos para las personas que puedan derivarse de su mal uso.
- Difundirlos, derivarlos a terceros o utilizarlos para usos no autorizados.
- No eliminarlos de forma adecuada una vez ya no son necesarios.

Las empresas grandes, pymes, micropymes y autónomos, hemos de cumplir con el RGPD pero esto puede servir para reforzar también la seguridad en general de nuestro negocio, desde un punto de vista organizativo y tecnológico. Esto es posible si aprovechamos el momento para hacer una buena gestión de la seguridad, que incluya todos los aspectos de la privacidad mencionados.

Sinergias entre la gestión de la seguridad y el cumplimiento del RGPD

El Plan Director de Seguridad, en adelante PDS, tiene entre sus objetivos reducir los riesgos para las personas y las organizaciones del mal uso de los datos personales. El PDS, nuestro plan, nos ayudará a tener un sistema de gestión de la seguridad de la información en continua mejora y actualización. El RGPD obliga a las empresas a analizar los riesgos contra la privacidad y a mantener registros de sus tratamientos de datos personales. Estas son algunas áreas en las que existen sinergias entre PDS y RGPD:

- seguridad de los datos personales
- notificación de brechas de privacidad
- gestión de contratos con encargados del tratamiento
- registro de actividades de los tratamientos
- privacidad por diseño y por defecto
- derechos de los propietarios de datos

Tanto si tenemos ayuda externa para las tareas técnicas como si tenemos personal en plantilla, la siguiente tabla muestra algunas de las cuestiones que se han de tratar al poner en marcha el PDS para abordar a la vez el RGPD.

Área

Seguridad de los datos personales (Artículos 5.1.f, 32 y 39)

- ¿Qué tipos de datos personales se recogen, tratan y almacenan? ¿Son datos especialmente protegidos? ¿Protegemos estos últimos con seudonimización y cifrado?
- ¿Están documentados los controles y protocolos que aplican a datos personales? ¿Existen controles técnicos y organizativos específicos para cada categoría de datos y tratamiento?
- ¿Cómo se determinan las pérdidas de confidencialidad, integridad y disponibilidad? ¿Se realiza una evaluación de los riesgos para la privacidad?
- ¿Se cifran los datos personales en el almacenamiento y cuando se transmiten? ¿Tenemos capacidad de anonimizar y seudonimizar los datos personales?

Notificación de brechas de privacidad (Artículos 33 y 34)

- Para cada tratamiento de datos: ¿somos responsables o encargados?
- Los registros de los tratamientos, los inventarios de datos personales y sus métricas, ¿nos permiten identificar brechas de datos?
- Si tenemos DPO, ¿está incluido en los planes y procedimientos de gestión de incidentes?
- En caso de incidente, ¿tenemos controles específicos para mitigar los riesgos de las personas afectadas por brechas de datos personales?
- ¿Se ha incluido en los planes de respuesta a incidentes la notificación en 72 horas a las autoridades de control?

Gestión de encargados / responsables del tratamiento (Artículo 28)

- ¿Tenemos los datos y contactos de todos los encargados de tratamiento? Y si somos encargados de los tratamientos de otros ¿tenemos los datos y contactos de los responsables de estos tratamientos?
- Nuestra evaluación de riesgos, ¿contiene cuestiones sobre las medidas técnicas y organizativas para la protección de privacidad dirigidas a los encargados del tratamiento?
- ¿Hemos redactado las cláusulas contractuales que incluiremos en los contratos con terceros que vayan a actuar de encargados del tratamiento de datos personales?
- ¿Hemos revisado los contratos existentes con responsables de tratamiento anteriores para que incluyan estas cláusulas?
- Para cada tratamiento del que seamos responsables ¿requerimos a los encargados que nos pidan autorización antes de subcontratar a su vez el tratamiento?
- Para cada tratamiento del que seamos encargados ¿incluyen nuestras políticas de seguridad los requisitos del artículo 32 del RGPD?

Registro de actividades de tratamiento (Artículo 30)

Para cada tratamiento sabemos:

- ¿qué tipo de datos personales recogemos?
- ¿cómo y desde dónde se recogen los datos?
- ¿cómo y dónde se realiza cada parte del tratamiento?
- ¿cómo y a dónde se transfieren?
- ¿cómo y dónde se almacenan, protegen y borran?
- ¿qué políticas de retención y destrucción tenemos en marcha? ¿se siguen y revisan?

Privacidad por diseño y por defecto (Artículo 25)

- Qué datos personales son necesarios para cada tratamiento que gestionamos como responsables o encargados?
- Nuestras políticas actuales, ¿limitan la cantidad de datos personales que se pueden recoger, bien sea por diseño de los formularios o por otras medidas de seguridad?
- Si contratamos un equipo de desarrollo o adquirimos nuevas aplicaciones, ¿incorporan los principios de privacidad en los requisitos de diseño de nuevas aplicaciones?

Derechos de los propietarios de datos (Artículos 12, 13, 14, 15,16 y 17; Razones 63 y 64)

- ¿Hemos actualizado nuestros protocolos para informar a los propietarios de los datos y para recabar su consentimiento?
- ¿Tenemos procedimientos para clasificar e inventariar los datos de carácter personal y poder responder a las solicitudes de los usuarios sobre su información personal?
- Nuestros procedimientos actuales, ¿permiten a los propietarios de los datos acceder de forma segura a los datos personales que tenemos de ellos?, ¿tenemos otros datos personales a los que los propietarios no pueden acceder directamente?, ¿cómo se generan los informes sobre estos últimos y cómo se comunican de forma segura a los propietarios de los datos que lo soliciten?
- ¿Incluyen en nuestras políticas chequeos u otros procedimientos para revisar y corregir datos personales incorrectos o desactualizados?
- ¿Tenemos en marcha mecanismos para notificar a los propietarios cuando se modifican o se borran sus datos personales Art. 19 RGPD?
- ¿Utilizamos perfilado o toma de decisiones automatizadas basados en datos personales y los tratamos conforme al Art. 22 RGPD?
- ¿Tenemos en marcha procedimientos para no retener los datos personales más allá del tiempo necesario para el tratamiento o si el propietario decide ejercer su derecho de supresión? ¿Cómo se ejecutan y revisan estos procedimientos?
- ¿Disponen los encargados de la seguridad de la información y contactos actualizados sobre los terceros a quienes se transfieren los datos?

¿Que riesgos pueden suponer los asistentes inteligentes?

Fuente: Oficina de Seguridad del Internauta

Un asistente inteligente o IPA's (Intelligent Personal Assistant) es un dispositivo, programa o aplicación con el que una persona puede interactuar para realizar múltiples funciones automatizadas mediante un comando sonoro o visual.

Oficina de Seguridad del Internauta

Actualmente se pueden encontrar en el mercado multitud de asistentes personales que pueden ser configurados, tanto en dispositivos móviles como en dispositivos específicos (Google Home, Apple Homepod, Amazon Echo, etc.), como pueden ser Google Assistant, Amazon Alexa, Apple Siri, Samsung Bixby o el asistente de código abierto Mycroft entre otros.

Estos asistentes funcionan con las tecnologías de reconocimiento automático de voz o ASR (Automatic Speech Recognition), y de comprensión del lenguaje natural o NLU (Natural Language Understanding). La primera de ellas permite que el asistente inteligente reconozca la voz que escucha de forma pasiva, mientras que la segunda facilita la comprensión del mensaje que ha recibido. Aunque estas tecnologías han despegado de forma exponencial en los últimos años, vienen desarrollándose desde la década de los 50 del siglo pasado.

¿Qué tareas nos facilitan? Los asistentes inteligentes nos pueden ayudar a realizar una larga lista de tareas, consultar información online, realizar o recibir llamadas, escribir y enviar correos electrónicos así como recibirlos y leerlos, realizar listas de la compra, poner en marcha diferentes dispositivos electrónicos de la casa, etc.

Google Now Siri Cortana

No podemos olvidar que para personas con algún tipo de discapacidad (visual, auditiva, motora, etc.), estos asistentes, combinados con dispositivos médicos o robots, puede servirles de apoyo y mejorar su calidad de vida. Entre las ventajas que ofrecen para personas con discapacidad visual destacan la geolocalización, la lectura de pantallas e imágenes en aplicaciones del móvil o el reconocimiento facial, entre otros. Para personas de movilidad reducida, les permiten mediante comandos de voz realizar tareas como encender la luz, controlar la temperatura de una habitación o abrir una puerta. Para personas con discapacidad auditiva, destacan las aplicaciones que les permiten realizar y recibir llamadas de teléfono o configurar los audífonos a los diferentes niveles de sonido del ambiente en el que se encuentran. En el caso de personas con Parkinson, por ejemplo, les ayuda a controlar los espasmos de la enfermedad gracias a dispositivos conectados a una aplicación en su móvil.

FACTORES DE ATAQUE

Aunque son muchas las ventajas que nos proporcionan, también existen diversos riesgos relacionados con el uso de los asistentes inteligentes y los dispositivos conectados a ellos (electrodomésticos, enchufes inteligentes, etc.) si se produce el uso malintencionado por parte de terceras personas o ciberdelincuentes.

Por ejemplo, un asistente puede ser activado sin la clave de activación utilizando unas palabras o frases que fonéticamente se pronuncien de forma similar a dicha clave, y con ello se consigue operar con el asistente.

Los asistentes inteligentes pueden ser configurados para reconocer la voz de sus dueños y actuar sólo bajo las órdenes de sus voces, sin embargo, voces con entonación parecida, como puede ser un familiar o un animal que reproduzca voces humanas, como un loro, podrían llegar a interactuar con los asistentes. Además, los sistemas también pueden ser controlados desde fuera del domicilio donde se encuentran, por ejemplo, a través de un megáfono.

Estos factores podrían provocar que el asistente repita las últimas órdenes recibidas y acceder a datos como la agenda

o la lectura de un mensaje o correo electrónico, afectando así a su privacidad.

Otro problema que tienen los asistentes inteligentes es que pueden ejecutar órdenes recibidas mediante mensajes de baja intensidad sonora y mediante ondas electromagnéticas, imperceptibles por el oído humano pero que los dispositivos pueden capturar y ejecutar como si hubieran sido realizadas por una persona. Esto puede exponer la privacidad y la seguridad de una casa inteligente de forma grave, por ejemplo, si los ciberdelincuentes logran enviar un mensaje oculto al dispositivo o ejecutar órdenes como que se abra una puerta equipada con una cerradura electrónica o que todos los electrodomésticos se conecten a la vez.

También existe el riesgo de que cuando se dan órdenes complejas a estos sistemas, formadas por frases entremezcladas y repitiendo la fórmula de activación del asistente, un usuario malintencionado puede conseguir el acceso al mismo y ejecutar órdenes sin control en aquellas funciones que no estén protegidas mediante clave de acceso.

Para que comprendas hasta dónde puede llegar su uso y cómo se pueden explotar de forma malintencionada, vamos a exponerte dos ejemplos verídicos:

En un anuncio se pedía a uno de estos asistentes leer la definición de un producto tal y como estaba escrito en Wikipedia. Al decir un comando reconocido por el asistente, éste reprodujo la acción solicitada en los dispositivos de los televidentes.

En otro caso, el protagonista de una serie hizo un juego de palabras con el objetivo de que el asistente reprodujera la frase final que decía. Para ello repetía varias veces la palabra de activación entremezclada con otras frases hasta que los dispositivos que se encontraban en las casas de los espectadores reproducían la frase final.

CONSEJOS PARA SECURIZAR SU USO

Para evitar el uso no autorizado de dispositivos y asistentes inteligentes, te recomendamos tomar las siguientes medidas:

1. Configura el asistente para que sólo reconozca tu voz, o la de las personas que tú quieras, para evitar que otros pueda interactuar con él.
2. Desactiva las funciones que no uses, tanto en los asistentes como en los dispositivos conectados a ellos, para evitar que sean explotables por terceras personas.
3. Establece un código PIN para ejecutar funciones que puedan tener acceso a tus datos personales sensibles (contactos, planes, tarjeta de crédito/débito, etc.).
4. Aísla este tipo de sistemas en una red independiente junto con los dispositivos que utilizas para conectarte con ellos, móviles, relojes inteligentes, dispositivos IoT, etc. para evitar que alguien que acceda a tu red wifi pueda interactuar con ellos.
5. Protege todos los dispositivos como mínimo con WPA2 y contraseñas robustas. También es importante proteger la seguridad del router para evitar que alguien conectado a la red pueda acceder a él.
6. Cuando no utilices los dispositivos silencia el auricular/altavoz para evitar que se active de forma accidental. Para saber si el dispositivo está funcionando, puedes configurarlo para que procese un sonido con cada orden, como por ejemplo, un beep.
7. Mantén actualizado el software de los dispositivos, de los programas que incluye y el firmware.
8. Los asistentes inteligentes tienen configurado por defecto una palabra o frase de activación. Es recomendable que la cambies por otra diferente, aunque no todos los asistentes aceptan esta modificación.
9. Elimina cada cierto tiempo las búsquedas y órdenes que hayas dado a los dispositivos. Así evitarás problemas de privacidad, como por ejemplo que terceras personas puedan acceder a ellos.
10. No difundas en redes sociales interacciones con los dispositivos, la marca de los mismos y su geolocalización. Esto puede facilitar información que puede ser utilizada para realizar ataques de ingeniería social o contra el dispositivo.
11. Es recomendable que leas las políticas de privacidad de los asistentes y dispositivos para que sepas que información recolecta, almacena y comparte.
12. Usa el sentido común y no facilites información personal o confidencial a través de los asistentes.

Noticias

Países UE acuerdan posición sobre la normativa de ciberseguridad en las TIC

Los países de la Unión Europea (UE) aprobaron el pasado día 8 sobre el Reglamento de ciberseguridad, aplicable a los productos, servicios y procesos de TIC (tecnologías de la información y la comunicación), según informó esa institución.

El texto aprobado constituirá la línea que defenderá el Consejo (estados miembros) para alcanzar un acuerdo con el Parlamento Europeo (PE), colegislador en este ámbito.

La normativa sobre ciberseguridad pretende crear un marco de certificación a escala europea para los productos, servicios y procesos TIC, permitiendo a ese sector utilizar ese mecanismo por ejemplo para los automóviles conectados o los productos sanitarios inteligentes, informó el Consejo (países UE) en un comunicado.

En principio la certificación será "voluntaria", salvo que se indique otra cuestión en la normativa europea o de los estados miembros.

Además, la futura normativa prevé elevar la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) al rango permanente de Agencia de Ciberseguridad de la UE.

El ministro de Transportes, Tecnologías de la Información y Comunicaciones de Bulgaria, Ivaylo Moskovski, cuyo país preside el Consejo de la UE este semestre, afirmó que "este nuevo marco de certificación conseguirá aumentar "la confianza en la soluciones digitales innovadoras".

El marco de certificación de la ciberseguridad establecido por la UE será "válido" en todos los Estados miembros de la UE, de tal forma que para el usuario será "más fácil confiar en estas tecnologías" y para las empresas "más sencillo desarrollas su actividades a través de las fronteras".

Grande-Marlaska, nuevo ministro del Interior

Fernando Grande-Marlaska ha tomado posesión del cargo de ministro del Interior esta mañana en la sede del Ministerio del Interior en Madrid.

Durante este acto, Juan Ignacio Zoido ha hecho entrega de la cartera de Interior al nuevo responsable del Ministerio del Interior, Fernando Grande-Marlaska.

Formación

Formaciones de enfoque práctico sobre áreas y sectores de conocimiento de AECOC

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 (EPSI)**, 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

Promoción PortAventura Park 2018

La Dirección del parque de atracciones de PortAventura *https://www.portaventuraworld.com/*, como deferencia con nuestra Asociación, nos ha facilitado unos cupones de descuento (2x1) para distribuir entre nuestros Asociad@s (que serán concedidos por orden de petición y hasta fin de existencias).

Así, todos nuestros Soci@s que quieran disfrutar de esta promoción, pueden solicitarlo vía mail a la siguiente dirección: *secretario@adsi.pro*

Desde estas líneas agradecer a PortAventura su detalle, como ha hecho estos últimos años para con **ADSI** y recomendar a todos nuestros Soci@s y Amig@s una jornada lúdica en el parque, uno de los mejores destinos de ocio familiar de Europa y que proporciona experiencias inolvidables a familias y jóvenes en un entorno único, caracterizado por la aventura, la emoción y la fantasía.

Legislación

REAL DECRETO 355/2018, DE 6 DE JUNIO, POR EL QUE SE REESTRUCTURAN LOS DEPARTAMENTOS MINISTERIALES

PDF de la disposición en el siguiente enlace

REAL DECRETO 359/2018, DE 8 DE JUNIO, POR EL QUE SE CREAN SUBSECRETARÍAS EN LOS DEPARTAMENTOS MINISTERIALES

PDF de la disposición en el siguiente enlace

Revistas

Seguritecnia Nº 453. Mayo

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

- **Editorial:** El fin de ETA
- **Seguripress**
- **Especial:** Videovigilancia y control de accesos
- **Entrevista:** Ángel García Collantes. Decano del Colegio de Criminólogos de Madrid

Enlace: ver revista digital

Cuadernos de Seguridad Nº 333. Mayo

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:** «Security Forum, el gran foro tecnológico».
- **En Portada:** «Security Forum».
- **Entrevistas:** «Joan Balaguer, director comercial Grupo IPTECNO».
- **Artículos:** «De profesión, hacker».

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.