BOLETÍN Nº47 NOV 2022

AEINSE

Asociación Española de Ingenieros de Seguridad

Caos regulatorio y Buenas Prácticas...

AEINSE
Asociación Española de Ingenieros de Seguridad

Mensaje de la Junta Directiva

Pasan los meses, e incluso los años,
y nuestra profesión se desenvuelve en un cierto caos....

Caos regulatorio y Buenas Prácticas...

Las amenazas a empresas y ciudadanos no han parado de evolucionar, ni tampoco la tecnología de nuestra Seguridad que se les opone.

Pero mientras tanto una ley voluntariosa de hace 8 años regula genéricamente, más bien anuncia, cómo deben actuar las empresas de Seguridad y las empresas obligadas a protegerse. El intento de Reglamento que aún no se ha concretado en sus primeros textos, de hace 4 años, presentaba una disociación más que notable con la realidad.

En paralelo, parte de las amenazas, las de origen informático, se regulaban por otro camino y otro Ministerio, añadiendo complejidad a las empresas que tienen que atender dos frentes (a veces enfrentados).

La **legislación PIC (Protección de Infraestructuras Críticas)** fue un gran acierto en cuanto a tratar de forma conjunta las amenazas actuales, pero lamentablemente no se ha sido coherente con su existencia en las nuevas iniciativas legales.

Por todo esto, el que desde un punto de vista práctico, aprovechando las lagunas regulatorias, nuestro colectivo estudie y publique guías de buenas prácticas para proyectos e instalaciones es casi un deber. La **Ciberseguridad de los Sistemas de Seguridad**, la forma correcta de recepcionar un Sistema de Seguridad, la documentación de los Sistemas instalados, etc. son temas en los que marcar unas guías, de seguimiento voluntario en todo caso, puede ser de gran ayudad en estos tiempos confusos.

A los asociados de **AEINSE** que nos leéis, **os animamos a uniros en los Grupos de Trabajo** de desarrollo de estos temas (escribid a socios@aeinse.es).

Las **Buenas Prácticas**, reguladas o no, son parte de la solución al caos.

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

AEINSE estará presente en la mesa redonda sobre ciberseguridad que organiza la Fundación ESYS

10
NOV
2022

LA SESIÓN, QUE SERÁ PRESENCIAL, TENDRÁ LUGAR EL DÍA 10 DE NOVIEMBRE EN LA SEDE DE PROSEGUR

En ella intervendrán profesionales de ciberseguridad de **OCC (Oficina de Coordinación Cibernética del Ministerio del Interior), Endesa, AENA, Prosegur** y **AEINSE**. Nuestra asociación estará representada por **Alfonso Bilbao** que será el moderador y por nuestro compañero **Álvaro Ubierna**.

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

NUEVO GRUPO DE TRABAJO BUENAS PRÁCTICAS

EL OBJETIVO DEL GRUPO ES GENERAR DOCUMENTOS DE REFERENCIA EN LOS DIFERENTES TRABAJOS DEL DÍA A DÍA DE UN INGENIERO DE SEGURIDAD, EXCEPTO LOS QUE ESTÉN DENTRO DE LAS COMPETENCIAS DE LOS GRUPOS DE TRABAJO DE CIBERSEGURIDAD Y FORMACIÓN.

Estos documentos, que tendrán la categoría de guías desarrollarán actuaciones a realizar para asegurar la calidad del trabajo, el cumplimiento legal y las relaciones con los clientes. La creación de una determinada guía se realizará a petición de cualquier miembro de la Asociación, propuesta que, una vez analizada, debe ser aprobada por la Junta Directiva.

Los miembros de la Asociación interesados en participar en este grupo de trabajo pueden notificarlo al correo socios@aeinse.es.

+INFORMACIÓN aquí

GRUPO DE TRABAJO FORMACIÓN

Para ello, se ha comenzado a desarrollar el contenido de las áreas de formación: Gestión de Riesgos, Legislación, Normativa, Proyectos, Controles e Infraestructuras.

El trabajo está avanzado y se espera tener en este cuarto trimestre del año la publicación del documento.

GRUPO DE TRABAJO CIBERSEGURIDAD

El grupo de trabajo de Ciberseguridad ha reanudado su actividad tras el verano con el objetivo de lanzar un nuevo documento, la "Guía de buenas prácticas de gestión y mantenimiento de la ciberseguridad en sistemas de seguridad física", como continuación de la guía "AEINSE 10/21 "Guía de Buenas Prácticas de Ciberseguridad en proyectos de Sistemas de Seguridad Física" que tan buena acogida ha tenido en el sector. Esta Guía pretende orientar a los responsables de los sistemas de seguridad física para que las medidas de ciberseguridad que los protejan sean administradas y mantenidas adecuadamente.

Cabe destacar que los miembros del grupo de trabajo se han renovado, confirmando que se trata de un grupo dinámico en el que los socios de AEINSE interesados pueden incorporarse o retirarse en función de su disponibilidad y conocimientos sobre ciberseguridad en los sistemas de seguridad física.

Para este documento, contamos con el ingreso en el grupo de los socios Antonio Manzanares y Ramón Segarra a los que les agradecemos su disponibilidad y que junto con **Álvaro Ubierna**, **Alfonso Bilbao** y **Raúl Aguilera**, conforman el equipo que trabajará en esta nueva Guía.

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

Colaboración formativa de AEINSE con ACAES

Nuestros amigos de la **Asociación Catalana de Empresas de Seguridad (ACAES)** nos han invitado, a través de **nuestro Presidente Alfonso Bilbao**, a protagonizar una de sus "píldoras formativas" a sus asociados, en este caso sobre la posición de **AEINSE** en el tema de la **Ciberseguridad de los Sistemas de Seguridad Física**, objeto de una primera **Guía de AEINSE** sobre proyectos e instalaciones y de la elaboración, en marcha, de una segunda Guía sobre gestión y mantenimiento de las medidas de Ciberseguridad instaladas.

Nuevo reglamento de Seguridad Privada

Los trabajos para la nueva redacción sobre el **Reglamento de desarrollo de la Ley de Seguridad Privada** siguen su curso en el Ministerio del Interior.

Desde la **Unidad Central de Seguridad Privada** se ha solicitado a **AEINSE** diferentes aclaraciones sobre la propuestas enviadas en 2018. Solicitud atendida puntualmente.

Colaboración de AEINSE con la revista SEGURITECNIA

Desde **Seguritecnia** se ha solicitado nuestra participación en el estudio de las candidaturas a sus premios anuales, participando nuestro presidente en el jurado.

A la fecha de este boletín ya se han realizado los fallos de todas las categorías

SEGURITECNIA

SCATI

SCATI estrena nueva sede corporativa

SCATI traslada sus oficinas centrales a una nuevas y modernas instalaciones en la Plataforma Logística de Zaragoza (Plaza), en un enclave estratégico para el transporte y la logística tanto nacional como internacional

Esta nueva sede corporativa alberga las oficinas de los servicios centrales donde se encuentra el equipo de I+D, fabricación, soporte técnico y los departamentos de administración, comercial y marketing además de albergar salas de formación, gimnasio para los empleados y un potente showroom desde donde la compañía realiza demostraciones *in-situ* a sus visitantes.

Dotadas con lo último en tecnología de vídeo y control de accesos, las oficinas centrales de **SCATI** son una representación real de cualquier instalación donde conviven y se gestionan distintos sistemas de seguridad: sistemas de incendios, control de accesos, reconocimiento de matrículas, protección perimetral, desde el Centro de Control que tienen situado en su showroom.

SCATI, que cuenta en la actualidad con diversas **delegaciones en Madrid, Sao Paulo** y **Ciudad de México**, está experimentando un crecimiento estable durante los últimos años que han impulsado este traslado.

Dirección:
Ronda del Canal Imperial de Aragón, 18
Plataforma Logística Plaza · 50197 Zaragoza
Entrega de mercancías. Bari, 45

Johnson Controls-Tyco Security Products organizó junto a Idemia un evento focalizado en soluciones de biometría avanzada

18 OCT

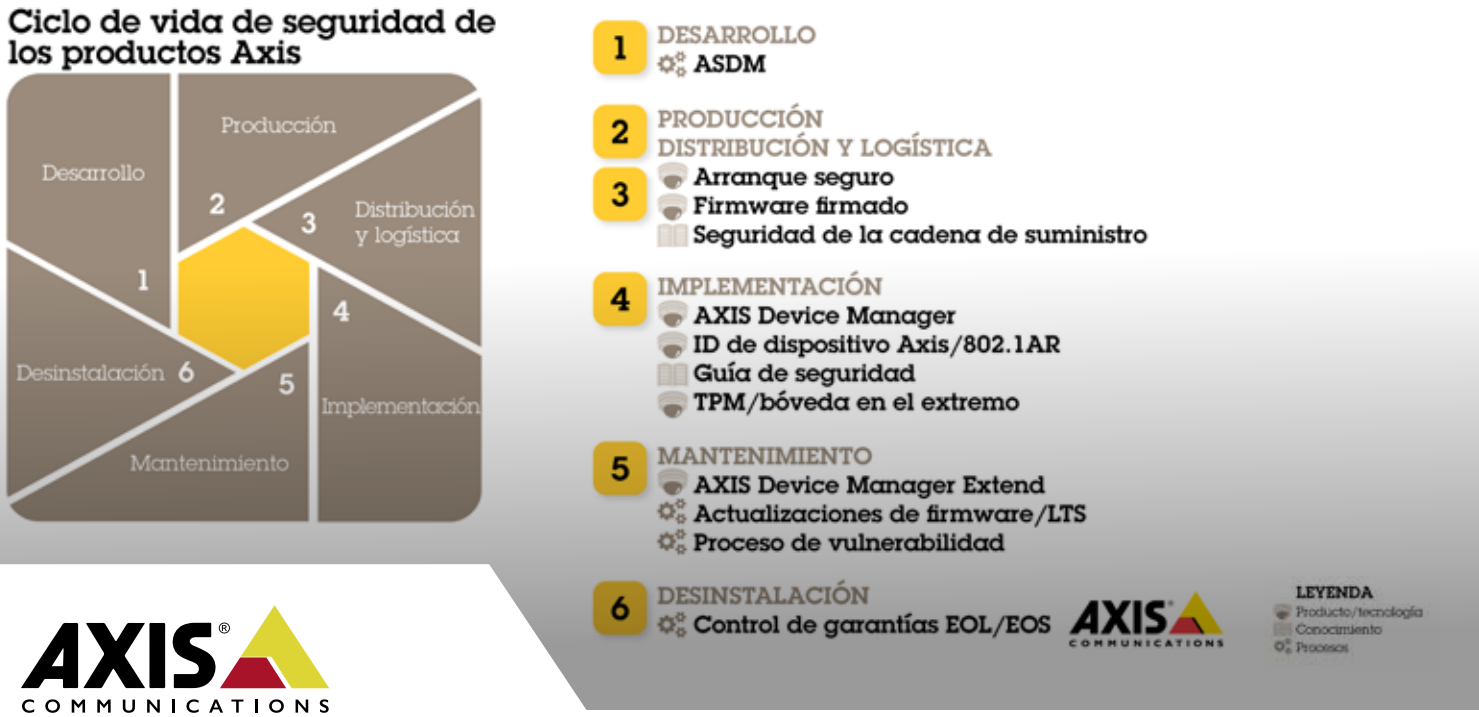
El pasado día 18 de Octubre Tyco Security Products e Idemia organizaron un evento conjunto en el showroom de Johnson Controls en Alcobendas (Madrid) en el que presentaron las novedades en biometría en control de accesos.

Idemia con una larga trayectoria en sistemas de identificación biométrica presentó durante el evento su lector de **huellas sin contacto MorphoWave**, dispositivo que permite compaginar la biometría de huella con los actuales requerimientos de higiene que se han vuelto más exigentes como consecuencia del COVID-19.

También se presentó la nueva versión MorphoWave SP que se trata de una versión simplificada pero que favorecen un menor coste por equipo. Además de biometría de huella se mostró el **dispositivo de reconocimiento facial VisionPass.**

Otro de los objetivos de la sesión fue demostrar la integración de los dispositivos de **Idemia** con la **solución de Sistema de Gestión de Seguridad de Tyco, C·Cure 9000.**

Gracias a dicha integración se permite al usuario final tener una experiencia perfectamente unificada sin tener que trabajar con dos sistemas independientes y gestionando desde un único interfaz el alta de usuarios, la detección de eventos, la automatización de BMS, etc.



AXIS COMMUNICATIONS

CIBERSEGURIDAD GARANTIZADA

DURANTE TODO EL CICLO DE VIDA DE LOS DISPOSITIVOS

La ciberseguridad ocupa uno de los primeros lugares en la lista de prioridades de cualquier organización. En un mundo cada vez más conectado, cualquier dispositivo conectado a la red representa un riesgo potencial para la ciberseguridad, y es imprescindible contar con un plan sólido para reducir esta exposición.

Los **dispositivos Axis**, con sus controles de ciberseguridad integrados, están diseñados para minimizar el riesgo de ataque e impulsar comportamientos seguros. Nuestro modelo pasa por aplicar las mejores prácticas de ciberseguridad a todas las políticas, procesos y tecnologías, desde la fase de desarrollo hasta su desinstalación.

La clave de la ciberseguridad es gestionar los riesgos. Hay que entender cuáles son, tomar decisiones activas para gestionarlos e implementar las prácticas recomendadas en el sistema. Como proveedor, asumimos la responsabilidad que nos corresponde aplicando las prácticas recomendadas. Y ponemos también a su disposición pautas, tecnologías, herramientas y servicios para ayudarle a mitigar los riesgos cuando utiliza nuestros productos.

"La clave de la ciberseguridad es gestionar los riesgos"

+ INFORMACIÓN aquí

Certificación de seguridad IoT en las nuevas cámaras Flexidome 5100i

BOSCH

Bosch introduce la nueva serie de cámaras inteligentes Flexidome 5100i.

Los aspectos novedosos de esta cámara son la inteligencia artificial embebida basada en redes neuronales, con el lanzamiento del nuevo análisis inteligente de vídeo IVA PRO, y sobre todo, los factores relacionados con la seguridad de los datos, además, por supuesto, de los ya reconocidos Calidad de Imagen, Gestión del Flujo, Grabación y Resiliencia.

Bosch es el primer fabricante en recibir el certificado SMM, Security Maturity Model, **certificado que emite el Industry IoT Consortium IIC**, que se amplía y desarrolla en las certificaciones IEC y UL, y recibe igualmente la certificación IEC-62443-4, partes 1 y 2, y UL-2900-2-3.

La **norma IEC-62443** engloba todo el proceso holístico de la seguridad para los sistemas de control y automatización industrial (IACS), incluyendo las competencias del personal (capitulo 3), procesos y procedimientos establecidos (capitulo 2) y la responsabilidad del fabricante de tecnología (capitulo 4 y capítulo 2 de la norma UL).

Es en este último apartado donde **Bosch** obtiene las certificaciones, que incluyen, además de los procesos y definiciones en la creación y desarrollo de productos seguros, todo lo relacionado con las pruebas de penetración, obteniendo un producto seguro e inmune a cualquier intento de ciberataque.

LANZAMIENTO DE NUEVAS ACTUALIZACIONES DE WIZ MIND

IMPULSADAS POR LA TECNOLOGÍA IA

Dahua WizMind es una cartera de soluciones para proyectos que incluyen IPC, NVR, PTZ, XVR y cámaras térmicas que adoptan algoritmos de aprendizaje profundo. Este año, Dahua ha lanzado nuevas actualizaciones de WizMind, utilizando inteligencia artificial y enfocado en las necesidades del cliente.

APLICACIONES BASADAS EN HUMANOS

El **sistema panorámico de Dahua** está diseñado para escenarios panorámicos, como grandes superficies urbanas. Las funciones del sistema incluyen multitudes (radio de 30 m) y vehículos (radio de 125m), rastreando simultáneamente ambos. Además, su cámara PTZ o la tecnología EPTZ rastrean objetivos en movimiento. Ideal para reemplazar múltiples cámaras y ahorrar costos.

WizMind también ofrece **Human Metadata 2.0** con un algoritmo que ubica objetivos en escenarios como fábricas, plantas, etc. También incluye la tecnología de **Detección de EPIs**, que detecta el incumplimiento del uso de equipo de protección personal en el trabajo, garantizando la seguridad de los trabajadores.

APLICACIONES BASADAS EN VEHÍCULOS

La **Gestión de espacios de estacionamiento** muestra el estado del espacio de estacionamiento en tiempo real. Detecta hasta 12 plazas en interior. Para exteriores, su rango de detección depende de la altura de instalación: 80 vehículos (30 m); 30 vehículos (12m); y 14 vehículos (6-8m).

WizMind también proporciona Detección de estacionamiento ilegal. Cuando detecta uno, toma instantáneas y guarda los metadatos, como el número de matrícula, el tiempo de infracción, la ubicación, etc. Cubre una zona más amplia con su sistema dual-PTZ. Además, el PTZ puede reproducir audios de advertencia, paliando el estacionamiento ilegal.

APLICACIONES DE IMÁGENES TÉRMICAS

WizMind también ofrece Medición de temperatura industrial en todo clima posible. Los datos se almacenan en línea, permitiendo accesibilidad a los usuarios. Vinculando sus dispositivos a la cámara, los usuarios pueden inspeccionarlos. Ideal para escenarios como subestaciones, donde se debe monitorear siempre.

VIGIPLUS
SE CONECTA A LA PLATAFORMA CLOUD DE IOT

DESICO DA UN PASO MÁS EN LA INTEGRACIÓN DE TECNOLOGÍAS IOT. YA ESTÁ DISPONIBLE EL MÓDULO DE COMUNICACIONES DE VIGIPLUS CON LA PLATAFORMA DESICO-IOT-CLOUD, LO QUE DA AL SISTEMA LA CARACTERÍSTICA DE EMISOR DE INFORMACIÓN COMO SI SE TRATARA DE UN DISPOSITIVO IOT CONVENCIONAL.

DESICO®

Esta nueva característica de VIGIPLUS es muy interesante, porque proporciona la capacidad de enviar al cloud toda aquella información gestionada por el sistema de Centro de Control y que ahora, simultáneamente, se podrá recibir en otra plataforma de carácter personal (Smarphone, Tablet o PC). Hay multitud de aplicaciones que han sido demandadas reiteradamente, a modo de ejemplo, un caso típico son las neveras en una gran superficie o las de farmacia en hospitales que, por el valor del contenido, es importante la información temprana de avería del equipo de frio.

En general se considera muy interesante recibir información personalizada de determinadas señales integradas en el sistema principal. Como son: señales técnicas, alarmas críticas, averías o parámetros generales que indiquen el estado y disponibilidad del sistema.

Con esta nueva funcionalidad Desico completa todas las opciones de intercambio de datos, añadiéndose a la integración de Vigiplus con dispositivos IoT para la recogida de datos de sensores, la plataforma desico-iot-cloud y la implementación de la sensórica IoT en nuestra receptora ASR2100 para envío a CRA convencional.

Las soluciones de acceso domakaba elegidas para el edificio multi-inquilino del Centro empresarial Bilma

dormakaba

Este edificio de oficinas, obra del arquitecto cordobés Rafael de la Hoz y localizado en la zona de las Tablas en el norte de Madrid, emplazamiento elegido por muchas de las más importantes empresas españolas para ubicar sus sedes.

Inició a comienzos del año 2020 un proceso de reforma integral de sus 43.500 metros cuadrados de superficie total construida. El edificio está compuesto por dos grandes bloques longitudinales – prismas rectangulares – claramente diferenciados, con halles de entrada y recepciones independientes. Así mismo, estos dos bloques están unidos entre sí mediante un núcleo de comunicación vertical, de forma que pueden formar una única pieza.

DETALLES DEL PROYECTO

El proyecto de reforma del **edificio Bilma** requería de la implantación de sistemas para la mejora de la accesibilidad, así como otros medios de individualización del paso de los usuarios con el fin de controlar y monitorizar en tiempo real la ocupación del edificio. Las **soluciones Mobile Access** de control de accesos se adaptan a las necesidades de un complejo de oficinas multi-inquilino que sufre cambios constantemente y permite gestionar accesos de manera remota.

Poder acceder hasta las oficinas sin la necesidad de tocar físicamente ninguna puerta mediante soluciones de activación de apertura automática sin contacto, es un requisito obligado en un complejo que se adapta a los nuevos tiempos y debe cumplir los mayores estándares de calidad y seguridad. Todo ello con un diseño unificado y acorde a la nueva estética de edificio.

LANACCESS

El Hospital Clínic de Barcelona y su apuesta por la videoseguridad

ESTA INSTITUCIÓN PÚBLICA LLEVA MÁS DE 15 AÑOS APOYÁNDOSE EN LAS SOLUCIONES DE LANACCESS

El Hospital Clínic de Barcelona es una organización compleja que suma 200.000 m² de superficie. La componen una facultad de medicina, un centro de investigación y varios centros médicos distribuidos por la ciudad condal. Lo explica Amadeu Bergés, jefe de seguridad del Hospital Clinic de Barcelona.

Es impensable proteger un centro sanitario de gran envergadura sin un sistema integral de videovigilancia, dice Amadeu en este artículo: "*El apoyo en la tecnología nos ofrece mucha información con un coste sostenido".* Cuando el jefe de seguridad llegó al hospital hace 15 años, comenzó un proceso de modernización de equipos y procedimientos que dura hasta hoy. Empezó renovando el parque de servidores por equipos de **Lanaccess**. El jefe de seguridad dice: *"nos hemos encontrado [con los nuevos equipos] con una solución muchísimo más estable y muchísimo más robusta".*

LA IMPORTANCIA DE LAS INTEGRACIONES

"Las cámaras de 360° para mí son el descubrimiento" dice Amadeu. El software de**Lanaccess** permite seccionar la imagen circular, generada por esta tecnología, para mostrarla en una vista panorámica plana o en múltiples vistas.

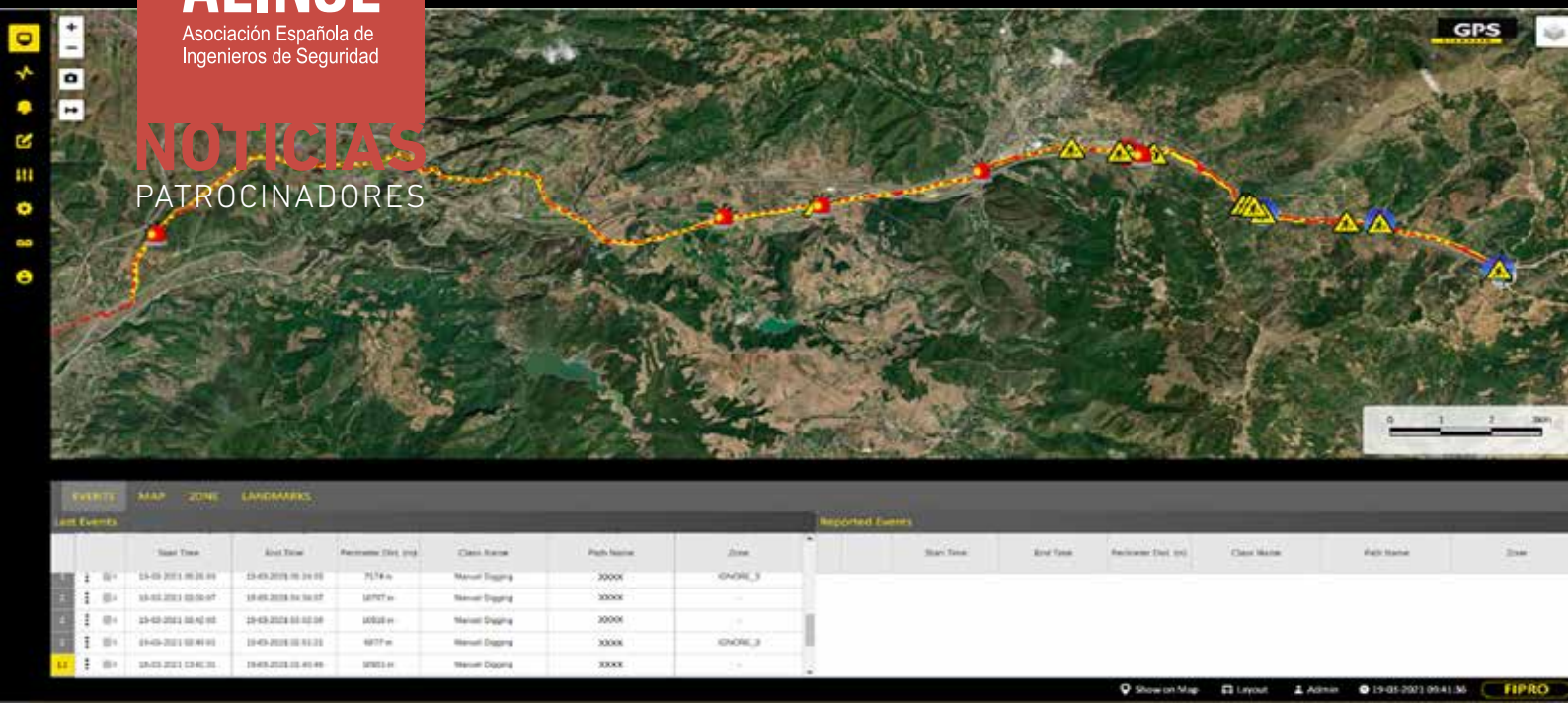
Otra integración parametrizada por **Lanaccess** la protagonizan los controles de acceso del fabricante **Dorlet**.

LA VIDEOANALÍTICA IMPULSA EFICIENCIAS OPERATIVAS

La videoanalítica no solo es útil para proteger las instalaciones, también para mejorar las eficiencias operativas porque permite controlar la afluencia de visitas y extraer datos estadísticos, como el tiempo de espera en consulta.

Lanaccess ayuda a los hospitales con una plataforma de videoseguridad completa, escalable e inteligente.

Entrevista a Amadeu Bergés,
Jefe de Seguridad del Hospital Clinic de Barcelona aquí



Sicuralia

DETECTOR POR FIBRA ÓPTICA DE LARGA DISTANCIA

HASTA 100 KM DE DETECCIÓN

Sicuralia presenta el nuevo sensor de fibra óptica de tecnología DAS FiPRO con capacidad para detectar intrusiones hasta 100Km desde un único punto de control con una precisión de hasta 4 metros.

FIPRO utiliza un cable sensor de fibra óptica con una alta capacidad de detección, midiendo cualquier perturbación acústica que se produzca a lo largo de la fibra, sería como disponer de mil micrófonos distribuidos a lo largo de la longitud de un activo (cable, tubería, perímetro).

El sistema es totalmente inmune a las interferencias electromagnéticas y a las condiciones atmosféricas y no requiere alimentación eléctrica a lo largo del perímetro protegido.

La fibra óptica es la parte sensible del sistema **FIPRO,** y funciona como un sensor acústico distribuido (DAS), ya que es especialmente sensible a la tensión acústica producida durante los intentos de intrusión y sabotaje.

De hecho, los efectos acústicos alteran la propagación del haz de luz láser, a lo largo del cable de fibra óptica. Estos cambios son medidos instantáneamente por el analizador **FIPRO,**. **FIPRO,** también puede aprovechar los cables de fibra óptica ya existentes, es decir, los cables de comunicación de FO.

FIPRO, puede instalarse enterrado y en vallas para proteger tuberías, perímetros, fronteras, etc. No tiene elementos metálicos ni piezas y es totalmente inmune a interferencias electromagnéticas, ofrece resistencia de corte construida y una precisión de detección >95% por clasificación de inteligencia artificial (AI), entre otras numerosas prestaciones avanzadas.

Obtener más información aquí

Hanwha Techwin

HANWHA TECHWIN LANZA WISENET WAVE 5.0

Wisenet WAVE 5.0 amplía su enfoque para aprovechar el poder de análisis de la Inteligencia Artificial, la ciberseguridad, la usabilidad del sistema y las nuevas posibilidades de interactividad para administradores y usuarios finales.

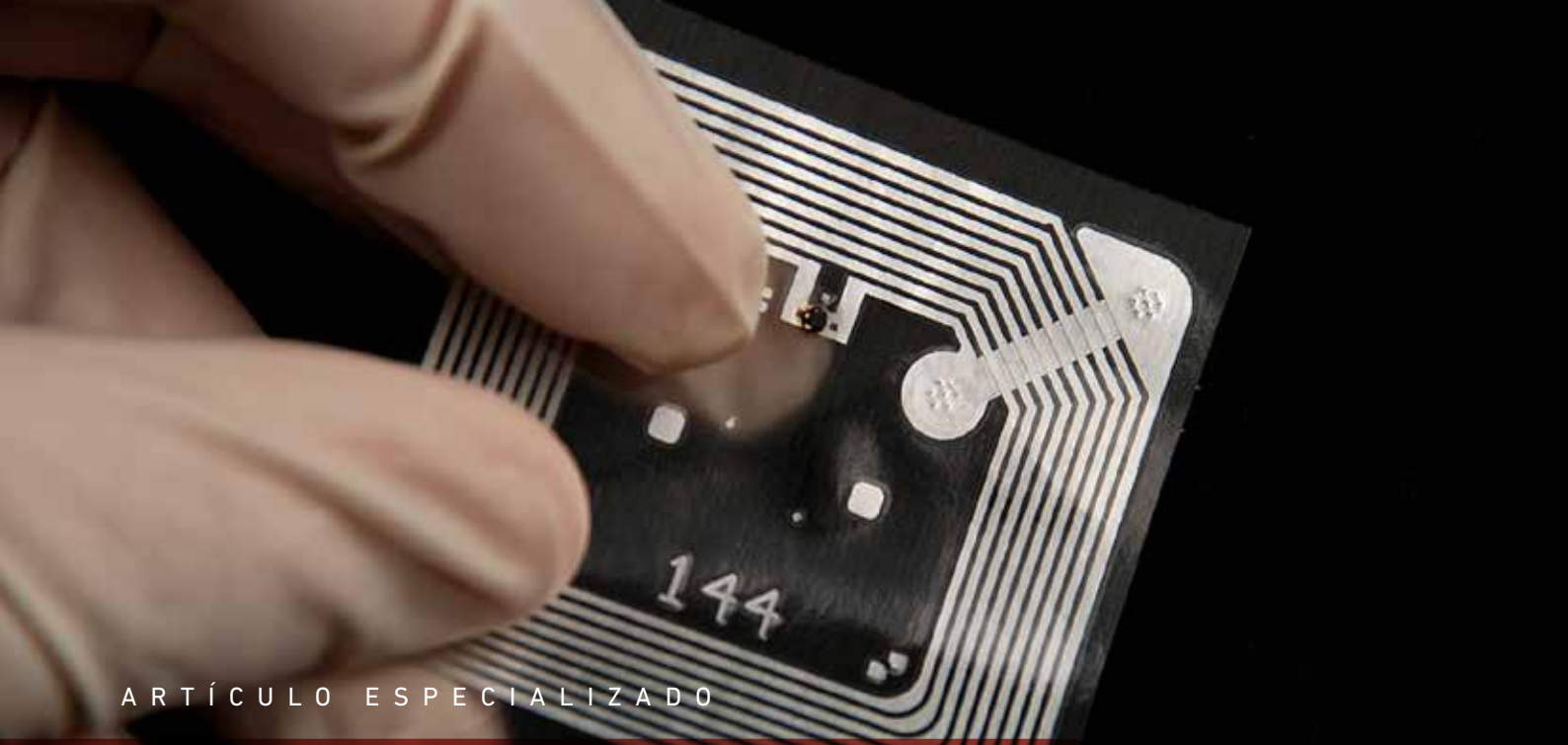
Los operadores podrán, de forma muy intuitiva mediante una nueva ventana, buscar objetos (personas o vehículos) por sus atributos específicos (color, accesorios, tipo de vehículo...). También será posible configurar copias de seguridad en función de esos metadatos generados.

En esta nueva versión se accede a funciones de reproducción más sencillas, para ver los últimos minutos de un evento. Así como información más detallada sobre los servidores y cámaras que graban un evento. El inicio de sesión se ha mejorado para ayudar al operador a ordenar, filtrar y ocultar fácilmente los sistemas.

La Ciberseguridad mejora con la autenticación de doble factor (2FA): opción que requiere que los usuarios utilicen una aplicación de autenticación para acceder (Google Authenticator, Microsoft Authenticator o Duo Mobile).

Las conexiones del Servidor utilizan ahora la fijación de certificados SSL/TLS, para evitar ataques de intermediarios. Además, Servidores y Clientes usan un nuevo tipo de autenticación basada en nueva sesión por defecto: los archivos de vídeo están cifrados y solo son visibles desde los Clientes.

+ información aquí



ARTÍCULO ESPECIALIZADO

TARJETAS DE PROXIMIDAD ¿SON REALMENTE SEGURAS?

Natxo Ruiz

JEFE ÁREA I+D HW DE DORLET

SI HABLAMOS DE TARJETAS DE PROXIMIDAD, SEGURO QUE CONOCES LA TECNOLOGÍA MIFARE®, TARJETAS DE MEMORIA PROTEGIDA Y DIVIDIDA EN SECTORES, SIMILAR A LAS CELDAS DE UN EXCEL, Y MECANISMOS SIMPLES DE SEGURIDAD PARA EL CONTROL DE ACCESOS.

Un producto **Mifare®** es básicamente un circuito integrado, lo que llamamos chip en lenguaje común. Con, aproximadamente, 250 millones de TISC (Tarjeta Inteligente Sin Contacto) y 1,5 millones de lectores vendidos, hoy en día es la más extendida por su rapidez y su bajo coste. De hecho, **el término Mifare® se usa ampliamente para designar cualquier tipo de producto RFID.**

Dentro de la tecnología **Mifare®** existe un extenso portfolio que ha ido evolucionando a lo largo de dos décadas de innovación. Desde el año 1994, que fue cuando nació la primera de ellas (**Mifare®** Classic), hasta el día de hoy, es un producto en continua evolución en cuanto a seguridad, capacidad y prestaciones.

Mifare® *Ultralight*

Tarjeta que nació en 2002, sobre todo pensando en ticketing. Ideal para aplicaciones de bajo coste y gran volumen que rápidamente comenzaron a sustituir a las ya obsoletas tarjetas de banda magnética o códigos de barras.

Dichas tarjetas, desde un comienzo, ya cumplían con la normativa internacional SO/ICE14443, que es utilizada por más del 80% de las tarjetas inteligentes sin contacto. Continuó con su evolución a lo largo de los años con los siguientes elementos, todas ellas basadas en una muy pequeña memoria de entre 40 a 144 bytes:

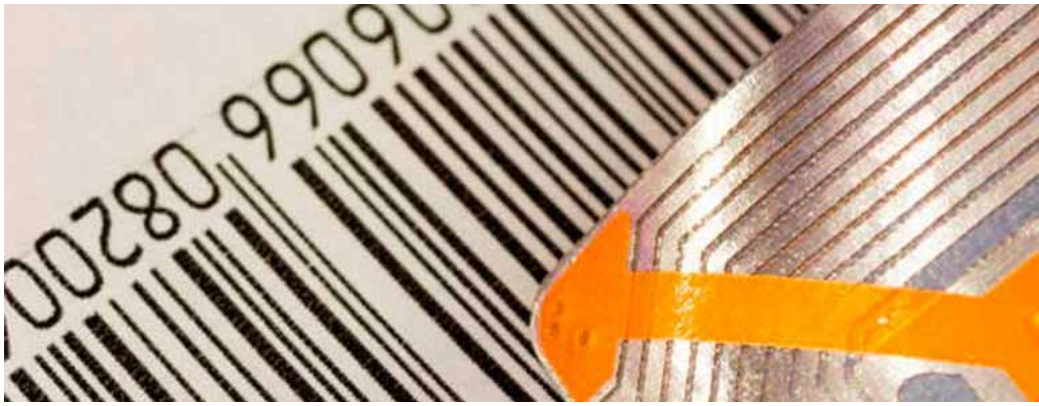
- **Ultralight Nano.**
- **Ultralight EV1.**
- **Ultralight C.**

La **familia Ultralight** hoy en día no es recomendable para nuevas instalaciones de control de accesos debido a su nivel de vulnerabilidad.

Mifare® *Classic*

Tarjeta con la que NXP salió al mercado en 1994 y que, a lo largo de estas dos décadas, ha ido evolucionando la familia.

Hoy en día, la familia **Mifare® Classic** es líder del mercado en cuanto a tarjetas inteligentes sin contacto. Al igual que el resto de las familias, opera en el rango de frecuencia de 13,56MHz cumpliendo la norma ISO/ICE14443A.



La tarjeta original dispone de una memoria de 1KByte, que se distribuye en 16 sectores. Cada uno de estos sectores se compone a su vez de 4 bloques de memoria de 16 bytes, siendo el último de ellos el lugar reservado para almacenar dos claves de acceso llamadas 'KEY A' y 'KEY B', junto con unos bytes de configuración. Mediante estos bytes es como se configuran los permisos de acceso a cada uno de los tres bloques. Estos permisos pueden ser: lectura, escritura, descuento o incremento (para bloques de valor).

Gracias a esta distribución de 16 sectores, se pueden llegar a tener 16 aplicaciones diferentes protegidas cada una de ellas con un par de KEYs diferentes.

Estas tarjetas envían al lector un código de identificación de conexión que usualmente es el número de serie de la tarjeta (CSN, Chip Serial Number), aunque la norma ISO 14443 dice que este número puede ser aleatorio. Con este número de conexión, **el lector está en capacidad de realizar cualquier operación en la tarjeta, previa presentación de las claves de acceso a los respectivos sectores.**

La ventaja de la tecnología Mifare®, como en cualquier otra tarjeta de identificación RFID, es que **no es necesario que tenga contacto físico para poder leer o codificar esta tarjeta chip**. También es destacable su facilidad de uso y que las aplicaciones basadas en tarjetas y lectores de tecnología Mifare® no requieren mantenimiento.

Su capacidad de cómputo no permite realizar operaciones criptográficas o de autenticación mutua de alto nivel, por lo que este tipo de tecnología está destinada a monederos electrónicos simples, control de acceso básico, tarjetas de identidad corporativas o de transporte y ticketing.

El problema actual de la tecnología Mifare® es que tiene un grado de vulnerabilidad bastante alto, ya que se pueden hackear y/o clonar de una manera relativamente sencilla. No se trata por tanto de un modo de identificación seguro para sistemas de control de accesos.

Sí que es cierto que, a lo largo de los años, esta tecnología ha ido evolucionando tanto en tamaño como en seguridad, pero la robustez y poca flexibilidad que proporcionaba la distribución de sus memorias han hecho que apareciera la **Familia Desfire®.**

Mifare Desfire®

Fue en 2002 cuando aparecieron las **tarjetas evolucionadas** de esta tecnología, con un grado de seguridad mucho más alto, denominadas **Mifare Desfire®**, que cuenta con hasta 4 versiones diferentes que hasta la fecha no se han podido clonar ni hackear:

- Desfire® (2002)
- Desfire®EV1 (2008)
- Desfire®EV1 256B (2015)
- Desfire®EV2 (2016)
- Desfire®EV3 (2020)

El nombre **Desfire®** se refiere al uso de cifrado de hardware DES, 2K3DES, 3K3DES y AES para proteger la transmisión de datos. **Este tipo de cifrado se considera uno de los más seguros e inviolables** y se utilizan para aplicaciones relacionadas con identificación del personal, control de acceso, fidelización, micropagos y transporte público o privado.

A diferencia de las tecnologías anteriores, estas tarjetas vienen **con funciones de seguridad avanzadas**, tales como mensajería segura y autenticación mutua, además de que se apoyan en **algoritmos criptográficos** modernos. También permiten una mejor protección de la privacidad de los usuarios, pues ofrecen la opción de restringir o hacer difícil el acceso a la información compartida sin autenticación.

Cada **tarjeta Desfire®** contiene un **número de serie UID único** que garantiza su singularidad y reconocimiento, codificado en 7 bytes.

Además del gran avance en cuanto a seguridad comentado, esta familia permite una distribución de memoria a demanda de cada aplicación. Lo que con las tarjetas CLASSIC, la necesidad de querer **un único Byte** obligaba a reservar 4x16(bloques) = 54 bytes de la memoria de esta, ahora esto ya no sucede.

Hasta la EV1 (incluida), el número de aplicaciones capaces de poder generarse en una tarjeta eran 28, y dentro de cada una de estas aplicaciones se podían generar un máximo de 32 ficheros. Dependiendo del tamaño de la tarjeta en cuestión (2/4/8KBytes), estos ficheros podían ser lo grandes que la propia tarjeta te lo permitiese.

Sin embargo, a partir de la EV2, el número de aplicaciones que se pueden generar son ilimitadas, manteniendo los 32 ficheros por aplicación.

Además, las tarjetas con chip **Mifare Desfire® EV2** y **EV3** tienen ventajas significativas sobre las tarjetas de tipo EV1.

- **Mayor nivel de seguridad.**
  El nivel de garantía de evaluación (Evaluation Assurance Level) de los chips EV2 y EV3 es de nivel EAL5+, mientras que el del EV1 es de nivel EAL4+.
- **Memoria más flexible.**
  El chip EV1 tiene un límite de 28 aplicaciones simultáneas, mientras que el EV2 y el EV3 no tienen límites sobre este tema.
- **Retención de datos hasta 25 años.**

Por lo tanto, y respondiendo a la pregunta que nos planteábamos al principio, aunque las tarjetas **Mifare® Classic** son las más utilizadas a nivel mundial, debido a su bajo coste y rapidez de actuación, en el mercado actual existe una tecnología estándar más avanzada y mucho más segura, la **tecnología Desfire® EV2** o **EV3**, y que debería ser la utilizada en los nuevos sistemas de control de accesos.

Además, técnicamente hablando, es posible no utilizar sólo el número de serie de la tarjeta (CSN) como identificativo de la tarjeta sino grabar el número de la tarjeta en una de las aplicaciones programadas en la memoria de ésta, encriptada y protegida en keys de seguridad, propiedad únicamente del gestor del sistema. Se hace automáticamente y de una manera sencilla al dar de alta una **tarjeta Desfire®** en un sistema de control de accesos tecnológicamente avanzado, dotando al conjunto tarjeta-control de accesos de una seguridad máxima.

Ésta sería por tanto la manera recomendada de funcionar en los nuevos proyectos de control de accesos a implantar en clientes con unos requerimientos de seguridad avanzados.

CONOCE A UN

SOCIO

Domingo Martínez Lacal

SOCIO Nº 140
dmlacal@gmail.com

Buenos días, Domingo, eres uno de los ingenieros veteranos de nuestra asociación. Para aquellos que no te conocen, por favor, "autopreséntate".

Nací en Dolores, provincia de Alicante, hace 65 años. Estoy casado y tengo dos hijos. Mi casa está en Alhaurín de la Torre, Málaga. Estudié ingeniería técnica industrial, en la Universidad Laboral de Tarragona. Al terminar el servicio militar, enero del 82, comencé a buscar trabajo y la primera empresa que respondió fue Fichet, no tenía ni idea de que iba eso de las alarmas, pero si había aparatos electrónicos de por medio... Dije que sí y hasta hoy.

¿Desde cuándo eres miembro de la asociación y por qué te asociaste?

Comencé a formar parte de la Asociación en 2014. Cuando Alfonso me hablo de la idea de formar la Asociación me pareció que era totalmente necesario disponer de una organización que nos represente, donde podamos relacionarnos, exponer nuestras necesidades, ideas e inquietudes que ayuden a mejorar el sector y nuestra profesión.

Además de la formación académica que ya nos has dicho, me consta que has hecho cursos formativos de otras actividades diferentes a la seguridad física. Dinos, por favor, los más representativos.

A lo largo de mi carrera profesional una serie de cursillos con el objetivo de completar conocimientos según las necesidades del momento.

Por ejemplo, cuando trabajé en mi empresa, Inde, tuvimos que trabajar en proyectos de iluminación para colegios e industria, todos estos proyectos debían disponer de cálculos justificativos y ajustarse a diferentes reglamentos, posteriormente los proyectos son visados por el Colegio Oficial de Ingenieros Técnicos Industriales de la provincia en la que se realizan los trabajos y además algunos de ellos serían inspeccionados por Industria para obtener la licencia de apertura. Por lo que tuve que realizar diferentes cursillos.

Uno sobre luminotecnia para el diseño de alumbrado público, alumbrado de centros deportivos y alumbrado de interiores. Impartido por JBC y PHILIPS. De forma que podíamos iluminar correctamente, aulas, salones de actos, pistas deportivas, etc. También hube que realizar instalaciones de alumbrado en casas rurales que no disponían de suministro eléctrico para lo que hice un cursillo sobre Cálculo de Iluminación con Placas Solares, impartido por BP Solar, donde te enseñaban a calcular la cantidad de placas solares y la cantidad de baterías y tipo de estas, según las necesidades de consumo de la vivienda.

Has pasado por diversas empresas en tu ya larga trayectoria profesional ¿puedes, por favor, hablarnos de ella?
Como mencioné anteriormente mi primer trabajo fue en Fichet, en Murcia, del 82 al 85. Empecé como técnico de instalaciones y mantenimiento de sistemas de detección de intrusión, CCTV, detección y extinción de incendios y algo de seguridad física.

Después, junto con dos amigos, montamos una empresa Instalaciones de Electricidad y Electrónica S.A.L. (Inde). Hacíamos proyectos e instalaciones de media y baja tensión, proyectos de naves industriales y sistemas de seguridad, fuimos subcontrata de Grupo 4 Securitas para toda la zona de Murcia y Alicante.

Me incorporé a Grupo 4 Alta Seguridad, para formar parte del departamento de proyectos en Madrid. Posteriormente fuimos Securitas y en el año 98 me traslado a Andalucía como delegado de Málaga, pasamos a llamarnos Securitas Sistemas y finalmente Niscayah.

En 2009 salgo de Niscayah, estoy un año en una empresa de iluminación led, Vendiled, un año en ADT Sensormatic y finalmente regreso a Securitas Seguridad España como delegado de Mobile en Málaga, Granada y Jaén gestionando los servicios de rondas, servicio de custodia de llaves y su comercialización.

Veo que prácticamente has estado en el sector de la seguridad y la protección contra incendios, excepto tu paso por el de la iluminación y la eficiencia energética ¿qué te llevó a moverte de nuestro sector?
Fue por casualidad, tengo conocimientos de luminotecnia y había hecho trabajos de iluminación vial y de interiores en Inde. En la entrevista de trabajo me presentaron un proyecto que comenzaba desde cero y se centraba en iluminación led y eficiencia energética. Debía ocuparme de la dirección técnica del mismo. El trabajo era muy atrayente. Fue un año muy intenso. Hicimos estudios para Puertos del Estado, hoteles, aparcamientos, etc. El mercado estaba muy verde, los clientes tenían cierta desconfianza, todo el producto venía de China y las inversiones iniciales eran muy fuertes. Empezaron a surgir problemas económicos y en dos años la empresa cerró. De haber tenido la empresa una economía más saneada, casi con total seguridad, me habría jubilado en ella.

Has hecho instalación, ingeniería y gestión. De las tres actividades ¿Cuál ha sido la más gratificante y por qué?
Sin ninguna duda me gusta y me he sentido más cómodo en la parte de ingeniería e instalación y lo cierto es que he disfrutado mucho en el área de Mobile de Securitas combinando sistemas con medios humanos. Diseñas el sistema, lo construyes y te responsabilizas de su funcionamiento con tus propios vigilantes.

¿Cómo ves la evolución de la seguridad en Málaga? Me refiero a empresas y clientes ¿el mercado del sector doméstico sigue siendo tan fuerte como hace años?
Como ya sabes el sector económico más importante en Málaga es el de servicios y dentro de este uno de los más potentes es el inmobiliario. Este sector ha evolucionado mucho en los últimos años, hoy en día, cuando se construye una urbanización se proyecten controles de accesos con lectura de matrículas, sistemas de CCTV e implementan un servicio de vigilancia que complemente estas instalaciones, hace unos años esto era totalmente impensable. Por la tanto el sector inmobiliario sigue siendo importantísimo ya sean pisos de 50 m^2 o villas de 3.000 m^2. La mayoría de los clientes son conscientes de la necesidad de disponer de sistema de seguridad en su vivienda, aun existiendo un servicio de vigilancia en su urbanización.

Déjame salir por un momento del terreno profesional y, como en la canción, ¿A qué dedicas el tiempo libre?
Normalmente hago una o dos horas de ejercicio, andar principalmente. Me gusta mucho la fotografía, sobre todo de naturaleza. Escucho algunos podcasts sobre todo de historia, cine, leer, algún proyecto de bricolaje y viajes sobre todo por Andalucía. El ejercicio y la lectura son todos los días el resto según me apetece, sin llegar nunca a estresarme.

Vamos ahora a AEINSE. Estás participando en uno de nuestros grupos de trabajo. Háblanos de ello. ¿Cómo ves la experiencia?
Estamos preparando, junto con Álvaro Ubierna, una Guía de Buenas Prácticas de Proyectos de Seguridad Física donde se relaciona como acometer la realización de un proyecto desde el diseño inicial con el cliente y toma de datos, hasta su puesta en funcionamiento. Obviamente todo son recomendaciones. La gran mayoría de nosotros ya estamos siguiendo estas recomendaciones, pero tenerlas relacionadas en un documento ayudarán a otros compañeros con menor experiencia. Por otro lado, esta guía deberá ir modificándose con vuestras aportaciones y según vaya cambiando la tecnología.

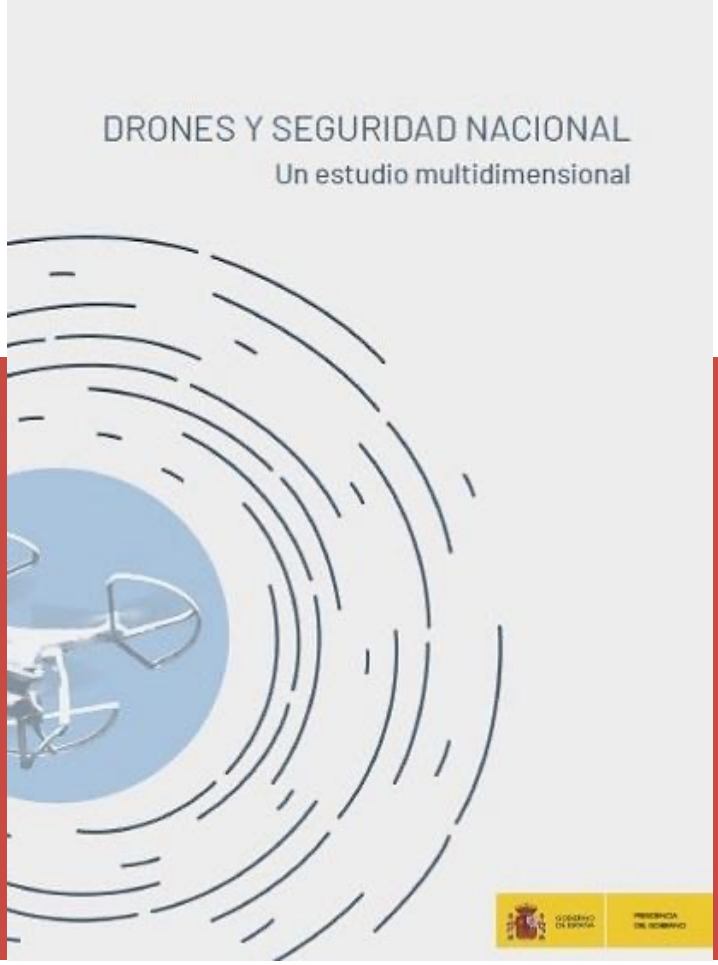
Ayúdanos a mejorar ¿Qué pedirías a AEINSE que propones que hagamos?
Pues me sumo a la sugerencia de Inmaculada Sanz sobre la colaboración con otras asociaciones de profesionales y universidades. Una gran mayoría de profesionales piensa que la seguridad es montar una alarma en la casa o colocar varias cámaras, que las contratan con que el que monta las antenas de TV.

Habrá que ver la forma de acceder a estas asociaciones y darles a conocer nuestro trabajo y lo que a ellos y sus clientes les puede beneficiar.

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS



El Consejo Nacional de Seguridad Aeroespacial (CNSA), órgano de apoyo al Consejo de Seguridad Nacional, publicó en julio 2022 el estudio ¨Drones y Seguridad Nacional".

El documento nace como respuesta lo determinado por la Estrategia Aeroespacial de 2019, determinando en su presentación *"La Estrategia de Seguridad Aeroespacial Nacional 2019 recoge entre sus líneas de acción impulsar el desarrollo normativo del uso civil de aeronaves pilotadas remotamente que garantice el necesario equilibrio entre la seguridad de las personas, instalaciones y demás usuarios del espacio aéreo, y el desarrollo tecnológico y económico de un sector pujante de la economía española".*

El estudio tiene ocho ejes de trabajo, entre los que se encuentran el relativo a la safety y security. Entendiendo esta última como la protección ante el uso malintencionado, incluso negligente, de los drones, convirtiéndose estos en una amenaza para la seguridad de los ciudadanos e instalaciones

Acceso al documento completo aquí

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

Feria Internacional de Seguridad, Defensa y Emergencias

Los días **17 a 19 de noviembre**, tendrá lugar en Silleda (Pontevedra) la **Feria Internacional de Seguridad, Defensa y Emergencias.** *"Primera cita a nivel nacional que reúna de forma conjunta y destacada a los principales agentes de cada uno de estos tres sectores clave en el desarrollo del bienestar y la protección social".*

INFORMACIÓN E INSCRIPCIONES

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

Proyecto de Real Decreto por el que se aprueba el Reglamento de Seguridad contra Incendios en los establecimientos industriales (RSCIEI)

REGLAMENTO SEGURIDAD CONTRA INCENDIOS

EL PASADO 22 DE OCTUBRE TERMINÓ EL PLAZO PARA PRESENTACIÓN DE ALEGACIONES A ESTE NUEVO REGLAMENTO, PRESENTANDO UN MES ANTES A INFORMACIÓN PÚBLICA POR EL MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO.

Este nuevo Reglamento sustituirá al anterior del año 2004 y presenta modificaciones en algunas disposiciones anteriores.

la nota del Ministerio *"Dada la evolución habida tanto en la técnica como en el marco normativo nacional y europeo, se hace conveniente revisar y actualizar los requisitos establecidos en el citado reglamento para adaptarlo a las necesidades y a las soluciones constructivas actuales, y al mismo tiempo, alinearlo con el resto de normativa de productos, instalaciones y edificación.*

En consecuencia, se hace necesario aprobar un nuevo Reglamento de seguridad contra incendios en los establecimientos industriales que regule las condiciones para establecer un nivel adecuado de seguridad en caso de incendio en los establecimientos industriales con carácter horizontal y de aplicación en cualquier sector de la actividad industrial".

El Ministerio tiene ya lo necesario para realizar el texto final. Habrá que estar atentos a su publicación

MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

Norma ISO 31030:2021

Gestión de riesgos de viaje. Orientación para las Organizaciones.

La norma fue publicada en septiembre del pasado año y, a pesar de su utilidad por las recomendaciones que realiza, creemos que no ha sido suficientemente divulgada ni considerada.

Según **ISO**, "Este documento proporciona orientación a las organizaciones sobre cómo gestionar los riesgos, a la organización y a sus viajeros, como resultado de la realización de viajes.

La norma da un enfoque estructurado para el desarrollo, la implementación, la evaluación y la revisión de:

- **POLÍTICA;**
- **ELABORACIÓN DE PROGRAMAS;**
- **IDENTIFICACIÓN DE AMENAZAS Y PELIGROS;**
- **OPORTUNIDADES Y FORTALEZAS;**
- **EVALUACIÓN DE RIESGOS;**
- **ESTRATEGIAS DE PREVENCIÓN Y MITIGACIÓN.**

Es aplicable a cualquier tipo de organización, independientemente del sector o tamaño, incluyendo pero no limitado a organizaciones comerciales, caritativas y sin fines de lucro, gubernamentales, no gubernamentales y educativas. No se aplica a los viajes relacionados con el turismo y el ocio, excepto en relación con los viajeros que viajan en nombre de la organización"

+INFORMACIÓN

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

Entre los informes publicados recientemente por la Secretaria de Estado de Seguirdad, se encuentra el IX Informe sobre la cibercriminalidad en España, correspondiente al año 2021.

Recoge los datos de los cuerpos policiales del territorio nacional (Cuerpo Nacional de Policía, Guardia Civil, Policía Foral de Navarra, Ertzaintza, Mossos d' Esquadra y Cuerpos de Policía Local que facilitan datos al Sistema Estadístico de Criminalidad).

- La criminalidad informática crece un **6,1%** respecto a 2020, registrándose **305.477 hechos delictivos.**
- El número de detenidos creció un **22,3%** respecto al año anterior
- En 2021 representa el **15,6%** del total de infracciones penales.

Por otra parte, incluye, entre otros, un interesante capítulo, el Nº2; Radiografía de la sociedad de la información, una serie de gráficos de situación de la sociedad española.

Acceso al documento completo aquí

AEINSE
Asociación Española de Ingenieros de Seguridad

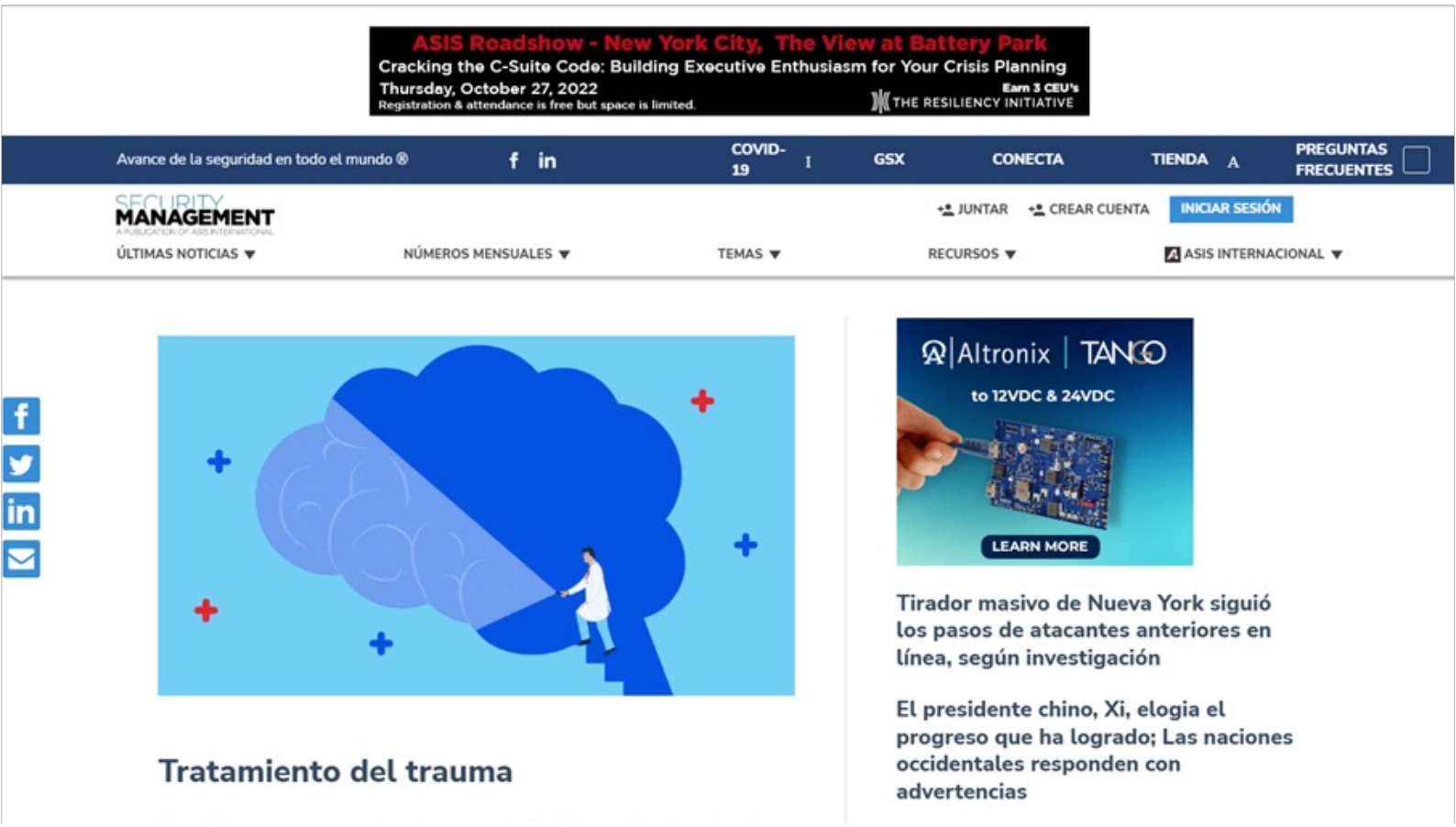
AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

Sistemas de avisos a la población y comunicación de la alerta temprana

ASELF y **Seguritecnia** organizan la jornada técnica **"Los sistemas de avisos a la población y la comunicación de la alerta temprana aplicados a la gestión operacional de las emergencias y catástrofes".**

Tendrá lugar los próximos días **7 y 8 de noviembre** y será en modalidad presencial, previo pago, en la **Escuela Nacional de Protección Civil de Madrid**.

Leer más



Security Management

EN LA PÁGINA DE LA REVISTA DE ASIS, SECURITY MANAGEMENT PODEMOS LEER UN INTERESANTE ARTÍCULO CON EL TÍTULO "TRATAMIENTO DEL TRAUMA".

"Cuando las personas experimentan un evento horrible, un desastre natural, un accidente automovilístico, un tiroteo, la muerte de un ser querido, su cuerpo emite una respuesta emocional conocida como trauma. Esto puede tener efectos adversos duraderos en la salud mental, física y emocional de las personas, así como en su bienestar social y espiritual".

Es algo que afecta, por ejemplo al entorno militar, policías, personal de emergencias, etc. El artículo da bastantes claves sobre ello.

Texto completo

LEÍDO EN...

CUADERNOS
DE SEGURIDAD

Leído en la web de Cuadernos de Seguridad...

El pasado 21 de octubre Patronal y Sindicados firmaron el **Convenio colectivo de Seguridad Privada**. Será efectivo desde 2023 al año 2016.

El convenio ha sido firmado por Aproser y Asecop, por parte de la patronal y UGT, CC.OO y USO por los sindicatos. Las organizaciones ELA y CIG han rechazado el acuerdo.

En el aspecto salarial, el convenio recoge un incremento del 6% para 2023 y sucesivos incrementos anuales hasta alcanzar el 16% en 2026.

Texto completo