BOLETÍN Nº54 DIC 2023

AEINSE

Asociación Española de Ingenieros de Seguridad

02 Mensaje de la Junta Directiva

03 NOTICIAS **AEINSE**
- Asamblea ordinaria AEINSE
- Trofeo Seguritecnia
- Formación ESSIIF-AEINSE
- Buenas prácticas biometría
- Sesión informativa
- Sicur 2024

10 NOTICIAS **PATROCINADORES**

21 ARTÍCULO **ESPECIALIZADO**
Drones
Pablo Serrano
Ingeniero de Diseño
Aurea Avionics

27 CONOCE A UN **SOCIO**
Benjamín Suárez

30 **AGENDA** DEL SECTOR

33 **LEÍDO, VISTO Y OÍDO EN...**

AXIS COMMUNICATIONS · BOSCH · casmar · alhua TECHNOLOGY · DESICO · DORLET · dormakaba · FFV GEUTEBRÜCK · Hanwha Vision · HID · Johnson Controls · LANACCESS · ISEO · Sicuralia · SCATI

AEINSE
Asociación Española de Ingenieros de Seguridad

Mensaje de la Junta Directiva

"Termina este 2023 y también un ciclo bianual más de nuestra Asociación, que deberá elegir a primeros de 2024 una nueva Junta Directiva"

Levantando la mirada...

Más allá de relatar aquí lo acontecido en este año queremos resaltar lo que debemos afrontar en el próximo ciclo 2024-2025, apoyándonos en lo realizado hasta ahora.

Lo primero de todo es celebrar nuestra **Asamblea Anual**, como en otras ocasiones coincidiendo con el inicio del **SICUR,** a finales de febrero. En ella pasaremos revista a lo realizado y, sobre todo, deberemos elegir una nueva Junta Directiva para el bienio.

Inmediatamente después participaremos en el **SICUR,** con presencia de un modesto stand donde podremos atenderos, además de una serie de actos que se están perfilando en la actualidad.

Pero levantando la mirada, y dependiendo de cómo quiera acometerlo la nueva Junta que salga de las elecciones, hay tres pilares importantes, trabajados en estos años, sobre los que fundamentar, al menos en parte, nuestro devenir:

- Seguir con el desarrollo de nuestra tarea formativa, empezando por los cursos desarrollados apoyando a otras entidades como **ESSIFF** o con las que se acuerde en el futuro y, sobre todo, haciendo realidad la oportunidad de los certificados conjuntos con **ISACA** para Ingenieros de Seguridad especializados en Ciberseguridad.
- Empujar nuestra actividad de generación de **Guías de Buenas Prácticas** en general, que sirvan de asesoramiento a nuestro colectivo y de puesta en común del bien hacer en nuestra profesión.
- Estar atentos a la posible actividad legislativa en nuestro sector, para poder aportar sensatez en los temas tecnológicos sobre todo.

Estos pilares están asentados (el tercero en las pocas ocasiones que se han dado) pero no serán los únicos, sólo de nosotros depende nuestro futuro, y podremos generar otras bases más y otras formas de desarrollarlas.

En el interior de este boletín encontraréis algunas novedades sobre **AEINSE** que esperamos que sean de interés.

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

26
FEB
2024

Asamblea General Ordinaria y Elecciones a la Junta Directiva

El día 26 del próximo mes de febrero celebraremos nuestra Asamblea General. Como en años anteriores, se hace coincidir con la fecha de inicio de SICUR para facilitar los desplazamientos de nuestros socios que no residen en Madrid.

Se comunicará a los socios con antelación suficiente la hora y el lugar de celebración. Como es tradición, estará seguida de una cena en la que tendremos oportunidad de conversar y conocernos mejor.

Por otra parte, en 2024 corresponde la elección de la Junta Directiva, asunto que formará parte de la asamblea. Desde estas líneas os animamos a presentar candidaturas a la misma. El pasado día 13 de diciembre se envió a todos los socios el documento para la presentación de candidaturas.

Guía Biometría

Guía sobre el tratamiento de control de presencia mediante sistemas biométricos

La reciente publicación de la *"Guía sobre el tratamiento de control de presencia mediante sistemas biométricos"* publicada por la **Agencia Española de Protección de Datos - AEPD**, pone sobre la mesa nuevamente el uso de los datos biométricos en otras aplicaciones.

Son muchas las preguntas a responder que, por otra parte, requieren interpretar las distintas publicaciones de la **AEPD**, el reglamento e, incluso, los documentos de la **Agencia Europea de Protección de Datos**.

¿Es la plantilla biométrica un dato de categoría especial?

¿Son únicas las plantillas de todas las tecnologías biométricas?

¿Permiten todas las tecnologías reconstruir la información biométrica a partir de la plantilla?

¿Cambia la plantilla biométrica con el crecimiento o envejecimiento de la persona, como con la geometría de mano?

¿Utilizan todas las tecnologías de biometría la inteligencia artificial en su aplicación?

Para apoyar la aplicación de la biometría en los sistemas de seguridad, con las garantías de privacidad en el tratamiento de los datos personales, AEINSE ha creado un GRUPO DE TRABAJO, dentro del área de BUENAS PRÁCTICAS, que tiene por objeto establecer directrices para interpretar el correcto uso.

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

GRUPO DE TRABAJO AEINSE

Buenas Prácticas

El **Grupo de trabajo de buenas prácticas** publicará antes de acabar el año la **guía AEINSE G34/23 Evaluación de riesgo y Proyectos de Seguridad**.

El objeto de esta Guía es definir los criterios que se deberán tener en cuenta para la realización de la Evaluación de Riesgos, como el proceso formal de un sistema de gestión de la seguridad basada en el riesgo y su necesidad e incorporación a los proyectos de seguridad.

Por otra parte, este grupo de trabajo tiene en proyecto la realización de diferentes guías que sirvan a los menos experimentados para acometer con éxito los proyectos, instalación, puesta en marcha y documentación de los distintos subsistemas utilizado en seguridad física.

Estas guías no podrán ser realidad sin la colaboración de los socios.

! Os hacemos desde estas páginas un llamamiento para colaborar en su redacción.

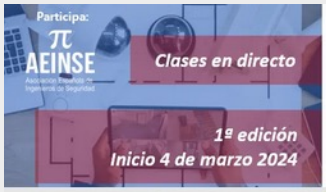
GUÍA AEINSE G34/23

Los socios interesados, envíad, por favor, un correo a
aeinse@aeinse.es
manifestando vuestro interés en participar en los GRUPOS DE TRABAJO.

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

Próximos cursos ESSIIF-AEINSE



Curso de especialización en sistemas de videovigilancia y CCTV

Aspectos legales, tecnología, diseño, implementación, pruebas y mantenimiento

Universidad Isabel I
Programa certificado

Área Seguridad
60 horas – 2,4 ECTS
Formación online

Curso de especialización en sistemas de control de accesos

Aspectos legales, tecnología, diseño, implementación, pruebas y mantenimiento

Universidad Isabel I
Programa certificado

Área Seguridad
60 horas – 2,4 ECTS
Formación online

Curso de especialización en sistemas anti-intrusión

Aspectos legales, tecnología, diseño, implementación, pruebas y mantenimiento

Universidad Isabel I
Programa certificado

Área Seguridad
60 horas – 2,4 ECTS
Formación online

En el marco del acuerdo de colaboración con el **ESSIIF** para la **formación de los ingenieros de seguridad**, en el mes de noviembre se ha llevado a cabo el **"Primer curso de Especialización en Sistemas Anti-intrusión"** con muy buena acogida.

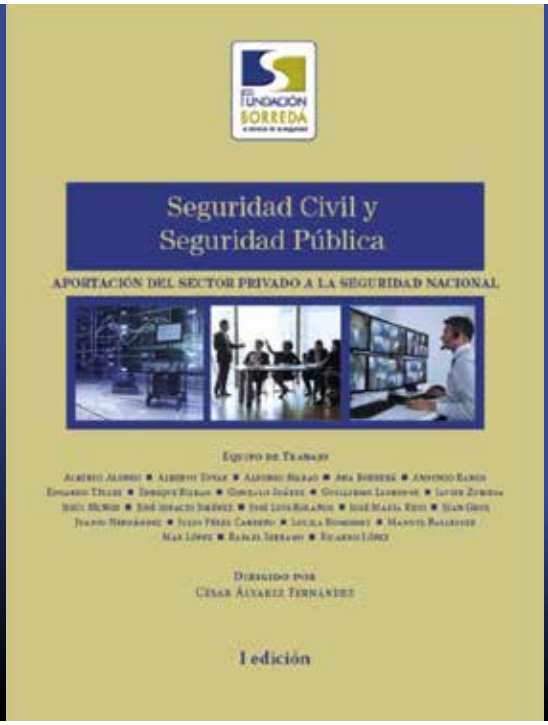
En 2024 y para continuar con el apoyo a la formación, están programados los cursos arriba andicados.

+información **aquí**

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

Seguridad Civil Seguridad Pública



La **Fundación Borredá** ha editado un interesante Estudio que bajo el título de **"Seguridad Civil y Seguridad Pública"** se constituye como un auténtico libro blanco sobre el sector de la Seguridad en un amplio sentido, afectando a la Seguridad frente a actos deliberados tanto en su vertiente física como de Ciberseguridad.

Para su redacción **se ha contado con un grupo de 22 profesionales**, entre los que se encontraba, en representación de **AEINSE**, nuestro Presidente, **Alfonso Bilbao**.

+información.

11 DIC 2023

Sesión informativa
sobre el grado de las instalaciones de seguridad

El pasado 11 de diciembre, y dentro del marco de colaboración con **AES (Asociación Española de Empresas de Seguridad)**, se realizó una sesión formativa sobre el contenido del documento de **AES "Guía de interpretación instalaciones grado 3 y 4"**, en la que se abordó la aplicación del cumplimiento de grado en las instalaciones de mayor complejidad, a partir de la interpretación de las **norma UNE-EN 50398** sobre sistemas de alarma combinados e integrados, y su aplicación durante la planificación, diseño e implantación, así como los apoyos sobre las **normas UNE-EN 50131, UNE-EN 50518, UNE-EN 62676** y **UNE-EN 60839.**

13
DIC
2023

AEINSE merecedora del Trofeo a la Formación en Seguridad de Seguritecnia

El pasado 13 de diciembre tuvo lugar la gala de entrega de la **36º edición de los Trofeos Internacionales de la Seguridad** de la revista **Seguritecnia**. En ella, y con una elevada representación del sector de la seguridad privada y autoridades, se reconocieron a los profesionales, empresas, entidades instituciones más destacadas durante 2022.

La **Asociación Española de Ingenieros de Seguridad (AEINSE)** ha merecido este año el **trofeo a la Formación en Seguridad** por su contribución a la formación de los ingenieros de seguridad. Su presidente, **Alfonso Bilbao**, y el responsable de formación de la junta directiva de la asociación, Iván Ballesteros, recibieron el premio entregado por **Pedro Antonio Ruiz**, director de la **Agencia de Seguridad y Emergencias Madrid 112.**

Iván, en sus palabras de agradecimiento, destacó el empeño de la Asociación en la transmisión de conocimiento, nexo de unión entre la tecnología, que crece de forma vertiginosa, y las personas. **AEINSE** , desde la publicación hace ya año y medio de su primera Guía, y movida por la amplia aceptación de la misma, apostó por seguir generando más guías de buenas prácticas y sesiones formativas encaminadas a difundir conocimiento a nuestros asociados.

+información.

SICUR
FEB-MAR
2024

AEINSE estará presente en SICUR 2024 con un stand de representación

La Organización de **SICUR**, como en la pasada edición, nos cede un stand para representación de nuestra asociación en este prestigioso evento internacional que el próximo mes de febrero **se celebrará entre el 27 de febrero y el 1 de marzo**.

Será un lugar de encuentro de los socios y, también un medio para dar a conocer nuestra asociación y su actividad a los visitantes de la feria y, en especial, a los ingenieros del sector.

También colaboraremos con la presentación de una ponencia en alguno de los actos que será anunciada en el momento que esté concretada.

Os esperamos en SICUR.

AXIS COMMUNICATIONS
BOSCH
casmar
dahua TECHNOLOGY
DESICO
dormakaba
DORLET
FFV GEUTEBRÜCK
Hanwha Vision
HID
Johnson Controls
LANACCESS
ISEO
Sicuralia
SCATI
AEINSE
Asociación Española de Ingenieros de Seguridad

Sicuralia

Sensor de radar ciberseguro Grado 3 MURENA COMPACT+

TECNOLOGÍA DE RADAR, DISEÑO COMPACTO Y MEMS INTEGRADOS

Sicuralia presenta el nuevo sensor radar de tecnología FSK combinado con el análisis Fuzzy Logic, MURENA COMPACT+, equipado con un sensor MEMS (Micro Electro Mechanical System) interno para una detección sofisticada de intentos de desplazamiento.

Selección dinámica de zonas

Gracias a la tecnología Fuzzy SRTD , Murena Compact+ puede excluir los movimientos cerca del detector, dejando un pasillo de paso libre, de tamaño ajustable, útil por ejemplo para patrullas cerca del edificio sin alterar el nivel de seguridad en la detección de intrusos que llegan desde el exterior, pudiendo seleccionar la dimensión del objetivo para discriminar los intentos de intrusión humana de vehículos en movimiento, animales pequeños, etc. Al mismo tiempo, es posible definir con una precisión de 1 metro el punto donde se desea interrumpir el área de análisis (Range Cut-off).

Compatible con IP READY, POE y dotado de Ciberseguridad

MURENA COMPACT + es "IP-Ready"

Con un solo cable ethernet se puede alimentar y gestionar de forma remota. La autenticación de protocolo cumple con el estándar de seguridad cibernética 802.1X, lo que permite a trabajar en una LAN segura, protegiendo los datos y equipos de los ataques cibernéticos, y ser gestionado desde los VMSs y PSIM mas populares como **Milestone, Lenel** o **Genetec.**

Nueva estructura y diseño

En un diámetro de unos 12 cm solamente, este pequeño radar incluye el protector superior para la lluvia, el paso interno de cables y un soporte especial incorporado, que permite una inclinación máxima de 75° en relación con la pared, inclinándose en todas las direcciones.

+información

SCATI

Scati Sentry

la plataforma de integración de sistemas

SCATI SENTRY unifica bajo una sola interfaz la información más relevante de todos los sistemas: CCTV, Control de Accesos, Intrusión, Detección Perimetral, Detección de Incendio, etc. pero también de otros relacionados con la gestión de un edificio como climatización o iluminación

SCATI SENTRY es una solución abierta, flexible y escalable que permite la interoperabilidad con otros fabricantes. Es capaz de rastrear y auditar todas las actividades y eventos para una posterior investigación de incidentes y permite crear procedimientos específicos de respuesta ante eventos que se produzcan en las instalaciones.

SCATI SENTRY simplifica la gestión diaria a los usuarios bajo una única plataforma y permite reducir tiempos de gestión, optimizar procedimientos y maximizar la rentabilidad del sistema.

Entre sus funcionalidades destacan:

- **ANÁLISIS AVANZADO** que permite detectar patrones de comportamiento sospechosos y eventos críticos en tiempo real a través de los análisis de datos.
- **AUTOMATIZACIÓN DE RESPUESTAS** ante eventos específicos para aumentar la eficiencia del sistema gracias a una acción coordinada de todos sus elementos.
- Proporciona herramientas para la **GESTIÓN DE INCIDENTES**, incluida la asignación de tareas, seguimiento y notificación.
- **INFORMES Y AUDITORÍA** para evaluar la eficiencia de los sistemas y cumplir con los requisitos normativos.

+ información.

AXIS COMMUNICATIONS

Intercomunicador para exterior

CON POTENTES FUNCIONES DE SEGURIDAD Y FACILIDAD DE INTEGRACIÓN

Axis Communications presenta un intercomunicador de vídeo y audio en red, compacto y potente que puede instalarse sin complicaciones en lugares estrechos. Este dispositivo para exterior incorpora funciones de ciberseguridad y admite la analítica avanzada basada en el aprendizaje profundo.

El **AXIS I8116-E Network Video Intercom** ofrece vídeo de 5 Mpx, comunicación bidireccional y control remoto de entrada. Con WDR (amplio rango dinámico), es garantía de imágenes claras cuando hay áreas oscuras y con mucha luz en la escena.

Con un tamaño de solo 48 mm de ancho, ofrece opciones de montaje ilimitadas. Puede instalarse en paredes, marcos de puertas y en un parteluz, y un accesorio especial permite el montaje empotrado en paredes.

Principales características:

- **Vídeo de alta calidad en 5 Mpx con audio.**
- **Compatibilidad con SIP para la integración del sistema de telefonía IP.**
- **Compatibilidad con analítica basada en el aprendizaje profundo.**
- **Funciones de ciberseguridad integradas.**

+información.

Para más información, póngase en contacto:
Maria Santafé, Segment Marketing Specialist Spain & Portugal
91.803.46.43
Maria.santafe@axis.com

Audio Analytics
mejorado por AI

BOSCH

Las cámaras FLEXIDOME panoramic 5100i son la primera serie con Intelligent Audio Analytics, lo que ayuda a comprender la situación de manera rápida para responder adecuadamente a un incidente.

Intelligent Audio Analytics detecta y clasifica los sonidos e identifica la dirección aproximada de la fuente. Esta nueva AI de audio detecta firmas de sonido de disparos, alarmas de humo (T3) y de monóxido de carbono (T4) al tiempo que ignora los falsos positivos, como portazos de automóviles o sonidos similares.

Esta detección precisa permite confirmar la alarma visualmente y actuar de manera proactiva. Las cámaras ofrecen una cobertura de 360 grados sin puntos ciegos, una matriz de micrófonos integrada y tres sensores acústicos **MEMS** *(Micro Electro Mechanical System)* que pueden capturar el sonido desde cualquier dirección para ayudar a guiar al operador al área de interés.

Las primeras licencias de software **Intelligent Audio Analytics** disponibles para las cámaras son **Gunshot Detector y Detector T3/T4** (alarma de humo y monóxido de carbono). Hay previstos detectores adicionales en futuras versiones de firmware.

Como todas las cámaras de **Bosch**, las nuevas cámaras panorámicas combinan AI incorporada con Internet de las cosas (IoT), convirtiendo fácilmente los datos de vídeo en información valiosa.

+información.

Dahua lanza DoLynk Care

para facilitar la transmisión de red

Dahua lanza sus propios switches gestionados en la nube para mejorar la transmisión de red. Estos switches ofrecen despliegue rápido, configuración sencilla, mantenimiento eficiente y transmisión PoE 2.0.

La integración con la plataforma en la nube **DoLynk Care** permite a los usuarios mantener de forma remota los sitios de sus clientes. Los dispositivos se añaden escaneando un código QR y se gestionan mediante la aplicación móvil o la plataforma web **DoLynk Care** . La plataforma identifica automáticamente los productos conectados y genera la topología correspondiente, facilitando la gestión unificada y la rápida implementación de dispositivos.

Los switches gestionados en la nube **Dahua** permiten la configuración remota de dispositivos, incluyendo funciones como reinicio, actualización, copia de seguridad y restauración. Además, ofrecen diversas funciones de gestión. En términos de mantenimiento, los switches **Dahua** ofrecen ventajas como la modificación remota de configuraciones, acceso remoto a cámaras IPC, panel de datos con información en tiempo real y diagnóstico de estado con un solo clic. También brindan funciones **PoE 2.0**, con un puerto que cumple con el estándar IEEE 802.3bt y salida PoE de 90W. Estos switches admiten **PoE Watchdog** para reiniciar cámaras problemáticas y ofrecen transmisión de larga distancia de hasta 250 metros, superando la limitación estándar de 100 metros.

En resumen, los switches gestionados en la nube **Dahua** ofrecen una solución de transmisión de red eficiente y conveniente, simplificando el despliegue, la configuración y el mantenimiento a través de una plataforma en línea unificada.

+información.

DESICO®

Cliente Vigiplus Cloud

Continuando con el proceso de desarrollo de prestaciones VIGIPLUS® en la nube y tras las presentaciones de Módulos en Cloud para gestión de visitantes, Control de Accesos o IoT, DESICO sigue avanzando por este camino, proporcionado nuevos productos basados en esta tecnología. En esta línea, se ha presentado recientemente un nuevo producto para VIGIPLUS, estando ya está disponible la versión Beta de un Cliente VIGIPLUS® gestionado íntegramente en Cloud.

Aunque VIGIPLUS® ya dispone de integración con dispositivos IoT y de conectividad para la exportación de información mediante esta tecnología a la plataforma de gestión IOT Cloud,

Este nuevo producto va a permitir a los usuarios de **VIGIPLUS®**, acceder como cliente ligero y mediante un navegador web, a sus proyectos de gestión de alarmas.

Esta integración se realiza a través de un software gestor de datos intermedio denominado broker, que reside en la nube en **plataformas AWS** o **Azure**, opcionalmente también puede implementarse en servidores locales, que evitan la conexión directa desde el exterior a nuestras estaciones de operador del sistema, lo que asegura una protección más, añadida a las políticas ya existentes de cifrado en las comunicaciones y de control de usuarios y permisos propios de la plataforma **VIGIPLUS®.**

Esta solución de cliente ligero para acceso a **VIGIPLUS®**., demandada reiteradamente por nuestros clientes, va a permitir acceder desde cualquier lugar a la supervisión de las instalaciones de gestión de alarmas, sin necesidad de instalación de software ni licencias, únicamente con un navegador web. En la línea de la innovación constante, **DESICO** apuesta por actualizar continuamente las herramientas de desarrollo. Con este objetivo los distintos módulos de la suite **VIGIPLUS®** se han adaptado para su uso con la última generación de nuestra plataforma de desarrollo.

+información.

Kaba exos 9300

Todo el control de accesos en un único sistema

dormakaba

La seguridad y la gestión eficiente de los procesos son fundamentales a día de hoy para cualquier empresa. Por ello, la necesidad de disponer de una solución que permita organizarse y administrar todas las aplicaciones de una manera fácil y flexible es cada vez mayor. Además, hay que tener en cuenta que ese sistema debe saber adaptarse a los cambios y el crecimiento que pueda experimentar la organización.

En este contexto, la solución de dormakaba, **Kaba exos** 9300, presenta como la solución perfecta. Con este sistema podrás resolver todas las tareas básicas de gestión de empleados, sistemas, usuarios y periféricos, e iniciar las medidas de seguridad específicas que sean necesarias.

Kaba exos ofrece una amplia gama de módulos escalables e inteligentes que se pueden adaptar fácilmente para satisfacer tus necesidades específicas, como la gestión de autorizaciones, la gestión de visitantes, la gestión de aparcamientos, el control de horarios y la asistencia, etc.

Además, se adapta a tu entorno informático actual y cuenta con interfaces abiertas y estandarizadas que permiten vincular fácilmente los distintos subsistemas para una transferencia de datos eficaz.

En definitiva, **Kaba exos** está diseñado para su uso a largo plazo y ofrece una total compatibilidad con el futuro y escalabilidad. Esto significa que el sistema crece contigo a medida que tus necesidades cambian, por lo que tu inversión siempre estará protegida en el futuro.

+ información.

Ciberseguridad de los Sistemas Geutebrück

VIDEOSISTEMAS FFV GEUTEBRÜCK

Los sistemas de grabación Geutebrück se distinguen por su compromiso prioritario con la seguridad y la integridad de los datos, respaldado por la implementación de protocolos de comunicación ciberseguros. Utilizamos el protocolo TLS para asegurar la comunicación entre cámaras y grabadores, mientras que los protocolos AES256, SAMBA y el estándar FIPS se encargan de la interacción segura entre grabadores y los puestos de visualización.

Nuestra estrategia de seguridad abarca un control exhaustivo de privilegios tanto de usuarios como de puestos de trabajo, respaldando el acceso por contraseñas sólidas y la gestión centralizada de derechos, actualizándolos en tiempo real de forma automática.

La integración con la gestión de dominios de Windows simplifica la asignación de derechos mediante grupos de usuarios y el práctico “inicio de sesión único”.

Para resguardar las imágenes, contamos con un formato de exportación propietario, diseñado especialmente para prevenir manipulaciones. Las imágenes pueden cifrarse y protegerse con contraseña, permitiendo incluso introducir áreas pixeladas. Todas las exportaciones incluyen cifrado y marcas de agua para garantizar la autenticidad, con opciones personalizables de almacenamiento.

La arquitectura de base de datos propietaria asegura el borrado de imágenes en el plazo seleccionado por el cliente, no permitiendo su recuperación posterior y garantizando el cumplimiento de la normativa vigente.

Hanwha Vision obtiene la certificación ISO 27001

Hanwha Vision ha obtenido la certificación ISO 27001, el estándar internacional para la seguridad de la información, reforzando aún más sus sistemas de gestión de seguridad interna (SGSI).

Para lograr esta certificación, una empresa debe pasar 93 controles en cuatro categorías: controles organizativos, físicos, tecnológicos y de personas. También requiere una mejora continua, con evaluaciones periódicas, para garantizar el cumplimiento. **Hanwha Vision** obtuvo voluntariamente esta certificación líder para reforzar sus defensas cibernéticas en toda la organización.

A medida que la tecnología avanza y aumentan los riesgos cibernéticos, la última versión de la ISO 27001 refleja las tendencias digitales cambiantes, como la nube, el **Internet de las Cosas** y la **Inteligencia Artificial**, para ofrecer un estándar que garantice la seguridad integral de la información.

Además, la compañía continúa enfatizando la importancia de la seguridad para respaldar las responsabilidades sociales, como parte de una campaña ambiental, social y de gobernanza más amplia, que coloca la tecnología y los datos en el centro de las operaciones.

Por último, destacar que la empresa ha sido seleccionada como organización **CNA** *(CVE® Numbering Authority)*, que trabaja con empresas tecnológicas líderes del mercado para gestionar posibles vulnerabilidades.

La **certificación ISO 27001** demuestra el compromiso de Hanwha Vision con la seguridad de la información, así como ser un socio fiable para sus clientes.

HID® Lanza su nueva gama de lectores Signo™ Express

Nos complace anunciar que estamos ampliando nuestra exclusiva línea de lectores HID Signo™ con la introducción de nuevos perfiles de lectores Express.

HID Signo Express es ideal para instalaciones que requieran un lector estrecho en puertas. HID Signo Express está diseñado para simplificar el proceso de selección.

HID Signo Express ofrece una configuración coste/beneficio muy rentable, combinando la compatibilidad de tarjetas físicas **HID Seos®** con la posibilidad de combinarlas con la **tecnología NFC** y/o **Bluetooth Low Energy®** para admitir **HID Mobile Access®**. Para su uso en aplicaciones específicas de baja seguridad, también está disponible una opción para leer credenciales con números de identificación únicos **(UID/CSN) ISO14443.**

Product Name	Part Numbers with Standard Key
HID Signo Express 20 w/ HID Seos + Bluetooth® Low Energy	20XTKK-X0-000000
HID Signo Express 20 w/ HID Seos	20XTKK-X1-000000
HID Signo Express 20 w/ HID Seos + CSN + Bluetooth® Low Energy	20XTKK-X2-000000
HID Signo Express 20 w/ HID Seos + CSN	20XTKK-X3-000000

Para más información sobre la línea de **lectores HID SIGNO Express**, puede comunicarse con su representante de **HID** o cualquiera de sus partners para realizar su pedido y analizar las necesidades de su próximo proyecto.

+información y contacto.

el nuevo portal de formación de

Johnson Controls Security Products

Johnson Controls Security Products se complace en presentar Tyco Learn, un nuevo portal de formación en línea que ofrece una amplia gama de recursos educativos para profesionales de la seguridad.

Tyco Learn es una plataforma interactiva diseñada para proporcionar a los usuarios acceso a videos cortos y simples que presentan las diferentes tecnologías, demostraciones de funcionalidades, manuales de instalación y configuración de los productos de Johnson Controls Security Products. Este portal abarca todas las marcas de la compañía tanto de vídeo como de control de accesos.

Con la creciente demanda de capacitación y formación en la industria de la seguridad, **Tyco Learn** busca facilitar el acceso a recursos educativos de calidad.

Los videos cortos y sencillos brindan a los profesionales de la seguridad la oportunidad de aprender de manera rápida y efectiva sobre las últimas tecnologías y productos de la compañía.

Además de los videos de formación, **Tyco Learn** ofrece acceso a los diferentes portales de soporte técnico que añaden una variedad de recursos adicionales, como documentos técnicos, guías de usuario, descargas de software, foros de consulta, preguntas frecuentes y la posibilidad de creación de solicitudes de soporte técnico.

Los usuarios pueden entrar en **Tyco Learn** en cualquier momento y desde cualquier lugar, lo que les permite acceder a recursos técnicos y aprender, a su propio ritmo y según sus necesidades.

Tyco Learn está disponible aquí

DRONES

Pablo
Serrano

INGENIERO DE DISEÑO
AUREA AVIONICS

pablo.serrano@aureaavionics.com

HOY EN DÍA, RARA ES LA SEMANA EN LA QUE UN DRONE NO OCUPE EL TITULAR DE ALGÚN MEDIO DE COMUNICACIÓN, PERO ¿QUÉ SON EXACTAMENTE ESTOS DISPOSITIVOS?

Terminología

La palabra **drone** es la que se usa con mayor frecuencia cuando se quiere hacer referencia a cualquier vehículo no tripulado, y aunque existen los drones terrestres y submarinos, son los aéreos los que más protagonismo tienen. En este contexto es posible leer o escuchar otra terminología como **UAS, UAV, RPA** o **RPAS**, por lo que es conveniente dejar claras las diferencias existentes entre estos acrónimos.

Un **UAS** (del inglés, *Unmanned Aerial System*) es un sistema aéreo no tripulado, entendiendo por sistema el conjunto formado por la aeronave, la estación de tierra desde la que se controla y el enlace de comunicaciones que hay entre ambas. A este tipo de aeronaves que no llevan tripulación se las conoce como **UAV** *(Unmanned Aerial Vehicle)*, y su control se puede llevar a cabo de varias maneras: autónomamente, dejando que la aeronave decida la ruta en función de la misión que se le haya establecido, mediante planes de vuelo pre-programados, o bien a través de un piloto a distancia, en cuyo caso se denominan **RPA** *(Remotely Piloted Aircraft)*.

Siguiendo este esquema léxico se tienen también los **RPAS** *(Remotely Piloted Aircraft System)*, que son sistemas aéreos cuya aeronave es remotamente pilotada por un piloto a distancia.

Y por último, mencionar también un término muy usado en este sector, y que se usará a lo largo de este artículo: carga de pago. En aviación, ya sea tripulada o no, la carga de pago la componen todos aquellos elementos que no sean usados para el propio vuelo y control de la aeronave, si no para cumplir con la misión que se le asigne. Es decir, la carga de pago es lo que le aporta valor al vuelo de una aeronave.

Si se trata de un vuelo comercial, la carga de pago la componen, entre otros elementos, los pasajeros y las maletas. En el caso de drones o aviación militar, la carga de pago pueden ser cámaras, **LIDARs** *(Light Detection and Ranging)*, sensores infrarrojos, radares, explosivos o ayuda humanitaria, entre otras.

Clasificación

Existen muchos factores por los que pueden ser clasificados los drones, por ejemplo: la misión para la que están destinados, la altitud máxima que puedan alcanzar, el número de motores que tengan, el medio en el que se desplacen, su grado de control o independencia del operador, el tipo de propulsión que usen, su peso máximo al despegue o su forma de volar.

De todos ellos, el peso es el más importante pues está directamente relacionado con el empuje necesario para el vuelo, el tamaño, la autonomía y la carga de pago que puedan portar. Es por ello que tanto el sistema de clasificación de drones de la **EASA** (Agencia de la Unión Europea para la Seguridad Aérea) como el de la **OTAN** se rigen principalmente por este factor. Como la **OTAN** solo tiene jurisprudencia en sus vuelos militares, este artículo se centrará en la clasificación y legislación que dicta **AESA**, que es la Agencia Estatal de Seguridad Aérea y está controlada y asistida por la **EASA**.

Normativa

Esta agencia distingue hasta siete clases de drones esencialmente según su masa máxima al despegue, aunque también se tienen en cuenta otros elementos como la velocidad y altura máximas alcanzables, el envío de telemetría al operador o el equipamiento de sistemas que mitiguen los daños a terceras personas. Además, también se establecen tres escenarios operacionales en función del riesgo que suponga la operación que se vaya a llevar a cabo. Entonces, cruzando las clases de drones con los escenarios operacionales es como se establece la extensa normativa existente en España y cada vez más unificada en toda Europa.

Llegados a este punto es importante destacar que esta normativa no es aplicable a las llamadas actividades no **EASA**, que son aquellas llevadas a cabo por servicios de aduanas, policía, búsqueda y salvamento, lucha contra incendios, control fronterizo, vigilancia costera o similares, emprendidas en el interés general por un organismo investido de autoridad pública o en nombre de éste. La normativa que regula estas labores en España es el **Real Decreto 1036/2017.**

En líneas generales, para volar un drone en España ya sea de manera recreativa o profesional, se deben cumplir una serie de obligaciones mínimas: registrarse como operador, formarse como piloto, obtener un seguro de responsabilidad civil, conocer la normativa y volar en lugares no restringidos como zonas militares, cercanas a aeropuertos o de protección medioambiental.

Drones como elementos de protección y vigilancia

Dada la extensa variedad de misiones que se le pueden otorgar a un drone, estos cumplen con creces con las funciones de proteger y vigilar, ya sea una urbanización privada, una frontera, un puerto marítimo o un elemento en particular. Pero, ¿cuáles son sus ventajas respecto a métodos de protección y vigilancia tradicionales?

Disponer de una cámara o un sistema de cámaras estabilizado en el aire y que pueda moverse en cualquier dirección y sentido supone grandes ventajas comparándolo con cámaras que se mantienen fijas en un punto. Esta movilidad permite hacer un seguimiento activo de cualquier punto que suscite interés, manteniéndolo en el centro del objetivo en todo momento incluso aunque se desplace y transmitiendo coordenadas en tiempo real a un operador o puesto de mando. Además, como consecuencia directa de dicha movilidad, también se pueden vigilar áreas que no dispongan de ninguna infraestructura de videovigilancia y/o que supongan un acceso muy complicado.

Otra gran ventaja es el poco tiempo requerido para desplegar un drone, del orden de unos pocos minutos, que junto a la transmisión de datos y vídeo en tiempo real suponen una rapidez de actuación que ningún otro dispositivo puede alcanzar. Ante posibles amenazas, su exploración mediante el envío de medios convencionales como un helicóptero o una patrulla suponen mucha más lentitud, además de altos costes económicos. También sería posible reducir o evitar el riesgo humano en acontecimientos en los que pueda haber enfrentamientos.

En el caso en el que se desee vigilar un perímetro, superficie o frontera, el uso de drones también está justificado pues son capaces de recorrer grandes distancias en muy poco tiempo e independientemente de la morfología del terreno, vegetación o si hubiera una gran superficie de agua. En este escenario, también sería posible vigilar la zona deseada por sectores o barrerla desde diferentes puntos de vista. En resumen, un drone supone al operador o cliente tener una cámara en cualquier punto, en cualquier momento.

El hecho de desplazarse en el aire hace que su entorpecimiento o saboteo sea mucho más difícil, pues es prácticamente imposible alcanzarlo de manera física, lo que sí puede ocurrir con cámaras fijas o vallas de seguridad que están siempre en el mismo lugar. Además, no se puede predecir dónde va a estar el drone de vigilancia por lo que el factor sorpresa siempre será un aliciente para el operador y un obstáculo para la parte observada. Un drone también puede brindar la oportunidad de operarlo de dos maneras: que sea indetectable, mediante el uso de hélices silenciosas, sin luces y manteniendo cierta distancia de seguridad, o bien que sea detectable, con el empleo de luces y altavoces, y actúe como instrumento disuasor.

Un aspecto interesante a tener en cuenta es que se pueden portar muchos tipos de carga de pago. Dependiendo del objetivo de la misión, de si es de día o de noche, si el cliente necesita una imagen muy nítida, si se requiere baja detectabilidad, etc, sin cambiar de drone se podría embarcar la cámara o cámaras más idóneas para el cometido del vuelo, altavoces, luces o un paracaídas, por ejemplo.

Aunque la diversidad de las cargas de pago haga frente a la variabilidad de las tareas de protección y vigilancia, es primordial por parte del operador escoger el tipo de drone adecuado porque existen grandes diferencias según la manera en la que generan sustentación. Principalmente hay dos tipos: de ala rotatoria si generan sustentación mediante el giro de dos o más hélices, o de ala fija si generan sustentación con alas fijas y al menos un motor, como un avión de pasajeros comercial.

Dada su naturaleza y de manera comparativa, los drones de ala fija pueden cubrir áreas extensas por su mayor duración en vuelo, son más silenciosos y tienen mayor velocidad de crucero; en cambio, necesitan un terreno adecuado para despegar y aterrizar, no pueden volar en estacionario y su control es mucho más complejo. Por otro lado, los drones de ala rotatoria o multi-rotores tienen más maniobrabilidad, se controlan de manera muy fácil y pueden despegar y aterrizar en terrenos complejos. Por tanto, será fundamental conocer correctamente los detalles de la labor a realizar, pues habrá una combinación idónea de drone, sistema propulsivo y carga de pago para ello.

Hasta ahora solo se han nombrado las ventajas que supone la incorporación de esta tecnología en la ingeniería de seguridad, pero no se puede terminar este apartado sin mencionar que dicha incorporación también supone una serie de desventajas a tener en cuenta. La primera de ellas es la autonomía, pues los sistemas tradicionales pueden funcionar de manera indefinida, mientras que un drone utilizado para estas tareas suele realizar vuelos típicamente de entre 20 y 50 minutos sin cambiar de batería.

La segunda de ellas es la complejidad que intrínsecamente tiene una operación aérea, pues se necesita de uno o varios operadores, formación, permisos de vuelo pertinentes, etc, que al final acaban suponiendo una barrera de acceso al uso de esta herramienta. Otro inconveniente, por ejemplo, es que siempre habrá que tener en cuenta la meteorología, pues juega un papel fundamental en las capacidades de un drone, pudiéndolas reducir y hacer imposible el vuelo.

Como se puede ver, los drones no han llegado a nuestras manos para sustituir a los sistemas de vigilancia habituales, pues cada escenario supone un reto distinto y estos no siempre constituyen la mejor solución. A día de hoy, lo más interesante es la combinación de los drones con los sistemas tradicionales, pues cada parte tendrá ventajas donde la otra no las tenga, suponiendo un bloque defensivo sólido, contundente y desalentador. Si se establece una buena coordinación entre ambas partes se pueden alcanzar resultados muy satisfactorios en la mayoría de circunstancias.

Drones como elemento de amenaza

Vistas algunas de sus bondades, hay que admitir también que esta tecnología es utilizada por grupos terroristas y paramilitares, bandas criminales y delincuentes tanto a alto como a bajo nivel para fines no legítimos. Dada la gran variedad de sensores o artilugios que pueden ser embarcados, sus aplicaciones son igualmente múltiples. Con una simple cámara se pueden grabar o espiar zonas con información sensible que pongan en compromiso la seguridad de un recinto, máxime si también se dispone de cámara termográfica o con la capacidad de aumentar el zoom óptica o digitalmente.

La obtención de datos sensibles con drones no solo se limita a lo que pueda grabar una cámara, si no que asimismo podrían obtenerse de múltiples formas, y todas de manera furtiva: embarcando dispositivos *Bluetooth*, generando redes *Wifi* maliciosas, escaneando tarjetas de acceso o monitoreando tráfico de red, entre otras.

El transporte y arrojo de material explosivo y productos químicos nocivos también son una práctica muy habitual, sobre todo en escenarios bélicos. En estos, además, son muy utilizados los drones suicidas, conocidos como munición merodeadora, que son drones diseñados para portar una carga explosiva y en lugar de soltarla, estrellarse con ella, provocando su explosión y por tanto eliminación tanto del objetivo como del propio drone.

Las zonas con baja densidad de población son el lugar perfecto para llevar a cabo el contrabando tanto de armas como de droga, aunque la capacidad de carga es limitada y por tanto no es un hecho corriente. Por esto mismo, para dar portes de alijos de droga son muy utilizados los drones submarinos, narco-submarinos o **UUV** *(Unmanned Underwater Vehicle)*, con una capacidad de carga y autonomía mucho mayor que las aeronaves no tripuladas.

Contramedidas y protección

Una vez alertados de la mayoría de los cometidos ilícitos que se pueden llevar a cabo con drones, se van a dar algunas pinceladas de contramedidas y protección contra drones pequeños que podrían utilizarse para atacar la seguridad física y privada, aunque por desgracia y al contrario de lo que se pueda intuir, no son demasiado esperanzadoras.

El empleo de plásticos en su construcción, su vuelo a baja altura y sus reducidas dimensiones dificultan sobremanera poder detectarlos mediante radares o a simple vista. Si se quisiera usar sistemas infrarrojos también se obtendrían pésimos resultados debido a la baja huella de calor que dejan a su paso. Tampoco pueden detectarse acústicamente, pues si se mantienen a una distancia prudencial, su ruido acaba siendo encubierto por el ruido ambiental. Queda claro que la detección, que es la primera contramedida ante una posible amenaza, es bien compleja. Pero el escenario no mejora si lo que se pretende es perturbar o entorpecer el vuelo de uno de estos drones. Para este caso, el mayor impedimento será el desconocimiento de la longitud de onda y el canal utilizado por el drone, que es información esencial para proceder con la perturbación ya sea inyectando información o coordenadas falsas, o bien negándole la localización GPS para dejarlo ciego.

Además, se debería utilizar un sistema cuyo uso no comprometa el correcto funcionamiento de sistemas propios, para lo cual será necesario tener la capacidad de realizar un análisis de sus frecuencias. Otra circunstancia a tener en cuenta es la potencia de la señal inhibidora frente a la de control, que será mucho menos efectiva si el emisor se encuentra cerca.

Como última opción, los drones también podrían ser repelidos con láseres, aunque tampoco son demasiado efectivos pues deben tener gran precisión en su apuntamiento (se recuerda que se trata de drones pequeños, volando a cientos de metros de altura), disponer de muy alta cadencia de tiro y disparar en cualquier dirección. Idealmente, tanto éste como cualquier otro instrumento deberían funcionar automáticamente y no depender de un operador.

Como se puede ver, hoy en día no existe una protección totalmente efectiva contra los drones, y por este mismo motivo son cada vez más las empresas dedicadas a estos menesteres, también conocidos como C-UAS *(Counter Unmanned Aerial System)* buscando una solución que pueda adaptarse al mayor número de escenarios posible. Ya que ninguna medida es 100% eficaz, de momento y a medio plazo, el gran reto de estas empresas será reducir el nivel de riesgo hasta cotas aceptables.

CONOCE A UN

SOCIO

Benjamín Suárez

SOCIO Nº 106

bsuarez@mapfre.com

Buenos días, Benjamín. Lo primero que te pido es que te presentes al resto de socios para que podamos empezar a conocerte.

Buenos días, Carlos. Nací en Madrid, hace ya 54 años. En esta ciudad he pasado mi infancia, he realizado mis estudios y desarrollado mi carrera profesional. Estoy casado y tenemos un hijo de 11 años.

¿Cuál es tu formación académica?

Estudié Ingeniería Técnica Industrial, especialidad en Electricidad, en la Universidad Politécnica de Madrid. Cuando comencé a trabajar en el mundo de la seguridad, realicé el curso de Dirección de Seguridad Privada, que en aquella época realizaba la **Fundación MAPFRE** junto con la Universidad Politécnica de Madrid. También cursé un Máster en Prevención de Riesgos Laborales en la **Universidad Carlos III de Madrid.**

¿En qué empresas, sectores y puestos has desarrollado tu actividad profesional?

Comencé trabajando como técnico de soporte y comercial en una empresa que distribuía equipos de RX para odontólogos.

Posteriormente, estuve un año y medio trabajando como responsable técnico de una empresa instaladora de protección contra incendios. Nótese el sinsentido de contratar para la dirección técnica a un joven sin ningún conocimiento ni experiencia en el sector. Este fue mi primer contacto con el mundo de la seguridad (safety), que ya no he abandonado en toda mi carrera.

Tuve que buscar información en libros, reglamentos, normas, etc. y pedir consejo a todo el que quería escucharme. Hay que tener en cuenta que Internet aún no se había popularizado. Fue una etapa dura, pero aprendí mucho.

En 1998 fui contratado por la extinta **SEGURMAP**, precisamente como especialista en instalaciones de incendio. Este fue mi primer contacto con la otra rama de la seguridad (security) y con **MAPFRE**, donde aún permanezco.

En 1999 se creó el **Departamento Corporativo de Seguridad de MAPFRE** y, como suelen suceder a veces las cosas, por casualidad, fui uno de los elegidos para iniciar esta aventura.

Esto me dio la oportunidad de vivir la creación desde cero del departamento. Desde el escrito a Seguridad Privada para su constitución formal, hasta la asunción progresiva de competencias: seguridad física, protección contra incendios, actuación en emergencias, CRA de empresa, ciberseguridad, continuidad de negocio, privacidad y protección de datos y gestión medioambiental.

Hasta finales de 2022 he ocupado diferentes posiciones relacionadas con el diseño y la gestión de instalaciones, tanto de seguridad como de protección contra incendios.

En noviembre de 2023 me ofrecieron ocupar una posición más gerencial, dentro de la Dirección Corporativa de Seguridad. Esto me ha dado la oportunidad de profundizar en otros campos, como la ciberseguridad, y la concienciación, sensibilización y formación en estas materias.

De las enseñanzas universitarias recibidas ¿Cuáles consideras que te han resultado más útiles en tu desempeño laboral?

De los estudios de Ingeniería, la formación de base en electricidad y, sobre todo, la capacidad de buscar soluciones a problemas complejos, de una forma sistemática.

Del curso de Dirección de Seguridad Privada, una visión global de la seguridad y un conocimiento profundo de la normativa y de las motivaciones y propósito de la misma.

Del máster de Prevención de Riesgos Laborales, el enfoque y metodología para los análisis de riesgos.

¿En tus veinticinco años en Mapfre cómo has vivido la evolución de la seguridad?

En estos 25 años, he asistido a una evolución de los riesgos de la compañía. En los años iniciales, nuestra mayor preocupación era un secuestro o atentado contra los altos directivos, tanto en España, donde eran objetivos potenciales de la banda terrorista ETA, como en LATAM, donde países como Colombia eran muy complicados. También sufríamos atentados, atracos y robos en nuestras instalaciones. Hoy en día, la seguridad de las personas sigue siendo nuestra principal preocupación, pero el cibercrimen supone el principal riesgo de las empresas aseguradoras, no solo de seguridad, sino global.

En cuanto a la tecnología, he vivido la enorme evolución de los sistemas. En los inicios, uno de mis cometidos era distribuir las cintas VHS para los videograbadores de las oficinas bancarias. He asistido a la revolución del vídeo y de las comunicaciones. Los sistemas de intrusión y de control de accesos, aunque han avanzado mucho, creo que aún tienen mucho margen de mejora.

En estos años has hecho proyectos, dirección de obra, consultoría, evaluaciones técnicas, gestión económica, etc. ¿Cuál o cuáles de estos trabajos te han parecido más satisfactorios?

Todas estas labores han sido gratificantes. Desde el punto de vista técnico, el diseño de sistemas es quizá lo que más permite desarrollar tu labor como ingeniero. Enfrentarte al papel en blanco es siempre un reto muy ilusionante. En la dirección de obra se aprende mucho de compañeros de otros oficios y requiere de gran flexibilidad y capacidad de adaptación.

En mi posición actual, lo más satisfactorio es poder trabajar en equipo con compañeros de diferentes países, así como con áreas muy especializadas en cada uno de los ámbitos de la seguridad. Esto me está permitiendo adquirir una visión más global y aprender temas nuevos todos los días.

De todos los proyectos en los que he participado, quizá el más complejo y, a la vez más ilusionante, fue la construcción desde cero de un nuevo centro de proceso de datos corporativo con certificación Tier III.

El actual crecimiento de las ciberamenazas está llevando a las empresas a dedicar recursos, tanto humanos como económicos, para protegerse de las mismas ¿Piensas que la ciberseguridad está desplazando a la seguridad física?

Realmente, no creo que la ciberseguridad esté desplazando a la seguridad física. El cibercrimen es una amenaza que hace 25 años, cuando comencé en este sector, era poco menos que ciencia ficción. Hoy en día, es el principal riesgo de muchas compañías, como comentaba anteriormente. Es lógico que las empresas dediquen recursos a protegerse.

En general, no tengo la percepción de que esto suponga descuidar la seguridad física.

Desde tu actual puesto de coordinación entre la Dirección Corporativa y las unidades de seguridad de los diversos países en los que Mapfre está presente ¿Encuentras diferencias en el modo en que se considera la seguridad en cada uno de ellos? ¿Existen diferencias notables en la normativa y legislación de los diferentes países?

La seguridad es en parte una percepción subjetiva. Es lógico que haya diferencias entre países con realidades y culturas muy diferentes.

En Asia tienen tendencia a colocar cámaras en número muy elevado, a veces, sin un propósito determinado. También encuentras lectores biométricos por doquier. En Europa somos mucho más sensibles con los aspectos de privacidad. En LATAM aún sigue primando la vigilancia con personas frente a los medios técnicos.

En cuanto a la normativa, España es un país hiper regulado, también en lo relativo a seguridad privada. Creo que no he encontrado ningún otro país con una normativa tan prolija y, lamentablemente, desactualizada.

Sin embargo, el mundo es cada vez más global y todas estas diferencias se van acortando. Europa lidera la legislación en privacidad, recientemente en materia de inteligencia artificial, pero cada vez más países tienen regulaciones que siguen esta estela.

¿Crees que las empresas emplean recursos suficientes en la sensibilización y formación de sus empleados en materia de seguridad?

Llevo solo un año como responsable de esta parcela y aun no tengo una visión suficientemente amplia para dar una respuesta fundamentada.

En el caso de **MAFPRE**, estamos realizando un esfuerzo muy importante en esta materia, tanto en la concienciación y sensibilización de todos los empleados, como en la formación especializada de los colectivos más sensibles.

Es una labor imprescindible desde el punto de vista de la prevención de los riesgos y, además, hay una presión creciente en esta línea por parte de grandes clientes, agencias de calificación y reguladores.

Sé que participas en algunos grupos de trabajo ¿Puedes hablarnos de ello?

Actualmente soy vocal del **Comité Técnico de Normalización 85** de **AENOR**. Esto me ha permitido participar en la redacción de la **Norma UNE 85160.**

Recientemente, me han invitado a participar en el **GT1 Cultura de Ciberseguridad,** dentro de **Foro Nacional de Ciberseguridad**, con el objetivo de elaborar una Guía para la seguridad física cibersegura. Es un proyecto ambicioso e ilusionante que me ha permitido reencontrarme con numerosos compañeros del sector, muchos de ellos, miembros de **AEINSE.**

Aparte de los temas laborales, que seguro te absorbe gran parte de tu tiempo, ¿qué aficiones son tu válvula de escape?

Me gusta pasear con mi familia, salir a cenar o compartir unas cervezas con los amigos. También acompañar a mi hijo en las actividades deportivas.

Mi gran pasión es viajar, aunque no puedo hacerlo tan a menudo como me gustaría.

¿Por qué te hiciste socio de AEINSE?

Coincidí en un **SICUR** con mi buen amigo y antiguo compañero de **SEGURMAP**, **Pedro de la Hoz**. Me contó la iniciativa y me apunté sin dudarlo.

¿Qué propondrías a la Asociación para mejor y aportar más valor a los socios?

Creo que son muy interesantes y necesarias las acciones para promover la formación de los ingenieros de seguridad.

En esta línea, creo que sería bueno promover algún tipo de certificación, que permita acreditar estos conocimientos.

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

La AEPD publica una guía sobre la utilización de datos biométricos para el control de presencia y acceso

Según la introducción las notas de la AEPD de introducción al documento, La Agencia considera el tratamiento de datos biométricos, tanto para identificación como para autenticación, como un tratamiento de alto riesgo que incluye categorías especiales de datos. Tal y como establece el RGPD, para poder tratar esas categorías es necesario que exista una circunstancia que levante la prohibición de su tratamiento y, además, una condición que lo legitime.

El documento fija los criterios para la utilización de la biometría para el control de acceso, tanto con fines laborales como no laborales, estableciendo las medidas que tenerse en cuenta para que un tratamiento de datos personales que utilice esa tecnología cumpla con el **Reglamento General de Protección de Datos (RGPD)** entre otras normativas.

La Guía precisa que, en caso de pretender captar datos biométricos, de forma previa al inicio del tratamiento, será obligatoria la realización de una **Evaluación de Impacto para la Protección de Datos** en la que, entre otros aspectos, se acredite la superación del triple análisis de idoneidad, necesidad y proporcionalidad del tratamiento.

Por otra parte, también establece restricciones en los tratamientos biométricos realizados para el control de presencia cuando se toman decisiones automatizadas sin intervención humana que tengan efectos jurídicos sobre la persona o le afecten significativamente de modo similar.

+ información aquí

VI Conferencia sectorial de Seguridad en Puertos

El pasado 14 de noviembre tuvo lugar en Madrid, con la colaboración de **Seguritecnia, Red Seguridad** y **Puertos del Estado**, la **VI Conferencia Sectorial de Seguridad en Puertos**. Evento en el que se abordaron cuestiones de interés encaminadas a mejorar la protección del ámbito portuario.

El acto fue inaugurado por la **secretaria general de Transporte y Movilidad del Ministerio de Transportes, Movilidad y Agenda Urbana, María José Rayo** y contó con representantes de diferentes áreas de **Puertos del Estado** y **Guardia Civil** que trataron diversos aspectos de la seguridad, como la ciberseguridad, las medidas de protección en el transporte de pasajeros y el control de fronteras entre otros.

Tras las ponencias sobre medios tecnológicos de protección desarrolladas por las empresas patrocinadoras, los **responsables de seguridad de los puertos de Tarragona, Almería** y **Barcelona** presentaron sus avances en la utilización de drones.

Puerto de Tarragona fue el pionero en su utilización, siguiéndole el de **Almería**. El de **Barcelona** empezará a desplegarlos el año próximo.

En el enlace a pie de página se accede a las ponencias de la **VI Conferencia Sectorial Seguridad en Puertos - Seguritecnia.**

+Información

VI Congreso de Seguridad Privada en Euskadi

El pasado 8 de noviembre se celebró con éxito el VI Congreso de Seguridad Privada de Euskadi. Organizado por Cuadernos de Seguridad y con la colaboración del Gobierno Vasco y SAE (Asociación Vasca de Profesionales de Seguridad).

El congreso fue inaugurado oficialmente por el **viceconsejero de Seguridad del Gobierno Vasco, Rodrigo Gartzia**. En su intervención destacó la capacidad del sector privado para *"aportar dinamismo para el sector público"* y *"contribuir a la seguridad colectiva y a la calidad de vida general"*.

En las distintas ponencias se abordaron temas de actualidad y visón de futuro como las estrategias proactivas basadas en la ciberinteligencia, la gestión del talento en las organizaciones del sector, la inteligencia artificial, el borrado seguro de datos, la utilización de drones, la evolución de delincuencia apoyada en la IA.

+Información

CUADERNOS DE SEGURIDAD

SUSCRÍBETE INICIAR SESIÓN

Impulsa Peldaño

CIBERSEGURIDAD VIDEOVIGILANCIA FUEGO INTRUSIÓN CONTROL DE ACCESOS SECTORES EVENTOS REVISTA EMPRESAS CLUB CS

Inicio > Fuego > Informe de la Fundación MAPFRE advierte sobre el récord de víctimas por...

Fuego | Protección pasiva

FUEGO

Informe de la Fundación MAPFRE advierte sobre el récord de víctimas por incendios en 2022

El año 2022 registró el mayor número de fallecidos por incendios en una década, destacando la importancia crucial de la prevención y la seguridad en el hogar.

"El año 2022 ha sido un año sombrío en España en lo que respecta a incendios y explosiones. Según el último informe de Víctimas de Incendios y Explosiones en España, elaborado por la Fundación MAPFRE y la Asociación Profesional de Técnicos de Bomberos (APTB), se registraron un total de 235 fallecimientos por incendio y explosión en todo el país.

Estas cifras superan con creces las de años anteriores y marcan un hito desalentador, habiendo duplicado su número en la última década".

+Información

LEÍDO, VISTO Y OÍDO EN...

GatesNotes THE BLOG OF BILL GATES

La IA está a punto de cambiar por completo la forma en que usas las computadoras

"Todavía me gusta el software hoy tanto como cuando Paul Allen y yo comenzamos Microsoft. Pero, a pesar de que ha mejorado mucho en las décadas transcurridas desde entonces, en muchos sentidos, el software sigue siendo bastante tonto".

Ver artículo

PATROCINADORES

AXIS COMMUNICATIONS
BOSCH
casmar
alhua TECHNOLOGY
DESICO
dormakaba
DORLET
VIDEOSISTEMAS FFV GEUTEBRÜCK
Hanwha Vision
HID
Johnson Controls
LANACCESS Discover the power of video.
ISEO ULTIMATE ACCESS TECHNOLOGIES
Sicuralia
SCATI