BOLETÍN Nº51 JUL 2023

AEINSE

Asociación Española de Ingenieros de Seguridad

02 Mensaje de la Junta Directiva

03 NOTICIAS **AEINSE**
Security FORUM
GT: Formación, Ciberseguridad y Buenas Prácticas
AXIS Cibersecurity Summit 2023

06 NOTICIAS **PATROCINADORES**

19 ARTÍCULO **ESPECIALIZADO**
Tratamiento de la ENERGÍA como Infraestructura Crítica
Ignacio Rojo
DORLET Security

26 CONOCE A UN **SOCIO**
Pedro de Ibarrondo

30 **AGENDA** DEL SECTOR

33 **LEÍDO EN...**

IA

La Inteligencia Artificial... ¿es Ingeniería Artificial?

AXIS COMMUNICATIONS · BOSCH · casmar · dahua TECHNOLOGY · DESICO · DORLET · dormakaba · FFV GEUTEBRÜCK · Hanwha Vision · HID · LANACCESS · ISEO · Sicuralia · SCATI · tyco

AEINSE
Asociación Española de Ingenieros de Seguridad

Mensaje de la Junta Directiva

"Inteligencia Artificial (IA) además de un tema central en la actualidad es también un término polisémico, significa varias cosas a la vez"

IA Inteligencia Artificial... ¿es Ingeniería Artificial?

Las aplicaciones para uso genérico como el famoso ChatGPT (textos), o fliki.ai(-videos), Autodraw (dibujos), Control net (dibujos y fotos), etc. son múltiples, y al alcance de aficionados, para bien y para mal (por ejemplo el uso de ChatGPT para generación de código de malware).

Quizá sea una parte muy popular de la presencia de la IA en la sociedad en general.

En nuestro gremio es bien conocida la existencia de **IA** por ejemplo en la gestión de la videovigilancia, ya sea a través del software inteligente embebido en las cámaras, o en la gestión de los VMS. También estamos acostumbrados a tratar con la **IA** en el ambiente doméstico, desde las máquinas aspiradoras hasta los ubicuos **Siri** o **Alexa.**

Estos ejemplos, sin duda irán planteando cambios en nuestras vidas de forma más o menos acelerada, y generando espacios inexplorados desde el punto de vista de la seguridad, la ética o la legislación.

Hay un conjunto de plataformas basadas en **IA** que, sin embargo, van a afectar en muy corto plazo de tiempo a nuestra profesión y a nuestros profesionales. Se trata de las plataformas especializadas en dotar de **IA** a tareas profesionales. Actualmente ya existen plataformas de ayuda al diagnóstico médico, de soporte a la gestión de los abogados, a la coordinación de operaciones militares, etc.

Se tata de que las tareas de recopilación de datos para inferir de los mismos decisiones (o ayuda a las decisiones) se realicen a través de estas plataforma de **IA**, y por ello se simplifique la actividad profesional.

Buscar una solución ante un determinado problema técnico de Seguridad, planteado en lenguaje convencional, hará que estas plataformas presenten alternativas sobre las que decidir, incluyendo los equipos necesarios o las tecnologías a utilizar.

Será, sin duda un acelerador importante a los proyectos o decisiones técnicas..., y también la posibilidad de no dedicar recursos a estas tareas.

¿Todo esto redundará en menos empleo? Puede ser. Pero lo que es seguro es que los Ingenieros de Seguridad han de conocer, manejar las nuevas herramientas que vienen e, incluso participar en su desarrollo, y que la **IA** no quiere decir **Ingenieros Artificiales**, sino que los Ingenieros de Seguridad reales manejarán la **IA** a su servicio.

Una vez más, la formación es esencial en el futuro, y el presente, de nuestra profesión.

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

Security FORUM

31
MAY
2023

El pasado 31 de mayo, y para celebrar el décimo aniversario de **Security Forum** , se celebró una cena institucional seguida de la entrega de distinciones a instituciones y asociaciones en agradecimiento al apoyo y colaboración con **Security Forum** durante sus diez años de actividad.

Ivan Ballesteros, a quien podemos ver a la izquierda en la imagen, recibió el galardón en nombre de **AEINSE.**

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

GRUPO DE TRABAJO
BUENAS PRÁCTICAS

A DÍA DE HOY SE ESTÁ TRABAJANDO EN LA REVISIÓN Y CORRECCIÓN DEL BORRADOR DE LA GUÍA G34/ 23 REALIZACIÓN DEL PROYECTO DE SEGURIDAD. ESPERAMOS PODER PUBLICARLA A PRIMEROS DE JULIO.

Las guías **G32/23 Análisis de Riesgos** y **G33/23 Diseño se encuentran en proceso de elaboración.**

A todos nos gustaría que la realización de las guías fuera más rápida, pero hay que tener en cuenta que los compañeros están trabajando y deben sacar tiempo libre para trabajar en ellas. Por esto, cuanto más se pueda repartir el trabajo, más rápido podremos avanzar. Si alguien se anima a colaborar puede enviarnos un correo a aeinse@aeinse.es

GRUPO DE TRABAJO
CIBERSEGURIDAD

El grupo de trabajo sigue trabajando en la revisión de la "Guía de Buenas Prácticas de gestión y mantenimiento de la ciberseguridad de sistemas de seguridad física".

Se espera su publicación para mediados del mes de septiembre. El verano es época complicada. Si alguno de los asociados estuviera interesado en incorporarse al grupo, puede ponerse en contacto con nosotros en la dirección de correo electrónico: **socios@aeinse.es**.

GRUPO DE TRABAJO
FORMACIÓN

EL PASADO MES DE ABRIL SE REALIZÓ LA SESIÓN FORMATIVA SOBRE INTELIGENCIA ARTIFICIAL Y LOS METADATOS EN EL ORIGEN DE LAS IMÁGENES.

Desde entonces el grupo de formación está preparando los temas de las próximas sesiones formativas:

- Las posiciones de cámaras más comprometidas y posibles soluciones.
- Aplicación del reporting como herramienta para reducir falsas alarmas.

Por otro lado, respecto a la publicación a principios de año del estudio **"AEINSE 21/23. Materias Formativas de los Ingenieros de Seguridad"**, se han recibido consultas por los grupos de interés sobre su contenido.

AXIS CIBERSECURITY SUMMIT 2023

El pasado 1 de junio tuvo lugar en la sede Microsoft de Madrid, el encuentro de AXIS sobre la ciberseguridad en sistemas de seguridad física. Bajo el lema "La ciberseguridad es una responsabilidad compartida" reunió a expertos de empresas proveedoras, usuarias, asociaciones y de la Administración.

01 JUN 2023

El evento tuvo **tres** paneles:

- La ciberamenaza a los sistemas de seguridad. ¿Por qué preocuparse y quién es responsable?
- Proactividad en ciberseguridad para los sistemas de seguridad ¿Cómo impulsar un marco normativo?
- ¿Cómo podemos trabajar juntos para reducir el riesgo?

En este último panel participó nuestro presidente **Alfonso Bilbao** que destacó dos conceptos en aras de reducir el riesgo:

- Formación de Usuarios, instaladores e ingenierías en la Ciberseguridad de los Sistemas de Seguridad como actividad ineludible.
- Implicación de los responsables de Ciberseguridad de las empresas usuarias en la protección de los Sistemas de Seguridad Física, considerándolos como Sistemas Informáticos a proteger, así como sus datos.

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

SCATI

SCATI VAS identifica códigos y realiza su seguimiento mediante cámaras de CCTV

SCATI VAS es el nuevo módulo software de análisis de vídeo que, a través de cámaras de videovigilancia, identifica y reconoce cualquier código, extrae su información y realiza un seguimiento del objeto o persona al que esté asociado.

Esta aplicación software realiza procesado de vídeo centralizado que permite a los usuarios disponer de motores de analíticas mucho más potentes y precisos que el procesado *on-the-edge* (en la punta).

Si bien la primera analítica incorporada en **SCATI VAS** está diseñada para detectar y reconocer **código de barras, QR, Datamatrix**, etc. en las imágenes capturadas por las **cámaras del sistema de CCTV**; nuestro **Departamento de I+D** ya está desarrollando nuevas analíticas.

Esta aplicación se integra con los diferentes módulos de la **SUITE VISION. SCATI VAS** identifica cualquier código en tiempo real, lo notifica mediante alarma a **SCATI WATCHER** y permite la visualización de imágenes asociadas a la alarma a través de un *pop-up*.

Paralelamente, los metadatos generados son recogidos por **SCATI RECKON,** el módulo de **Business Intelligence de SCATI**, que centraliza la información para facilitar las búsquedas a través de filtros personalizados o mostrarla de forma sintetizada a través de informes y gráficos personalizados.

Más información aquí.

AEINSE
Asociación Española de Ingenieros de Seguridad

tyco

Johnson Controls, Tyco Security Products presenta sus soluciones de Inteligencia Artificial y Radar en Security Forum 2023

Recientemente **Johnson Controls Security Products,** tuvo una participación destacada en el evento **del Security Forum**, celebrado los pasados días 31 de Mayo y 1 de Junio en Barcelona. Durante este importante encuentro, y formando parte de su propio **"Roadshow Europeo Sphere 2023"**, estuvieron presentes con su **camión de demostraciones MEU.**

Durante el evento se hizo la presentación de las **últimas soluciones de Inteligencia Artificial y de Radar,** tecnologías que combinadas permiten alcanzar los más altos niveles de eficacia en la detección perimetral.

Igualmente la tecnología de inteligencia artificial disponible en sus propias cámaras permite combinar reglas de analítica de vídeo y de categorización de objetos aplicables no solamente a entornos perimetrales, si no que a cualquier área donde se quiera realizar una detección avanzada. El camión de demostraciones MEU, ha sido el protagonista mostrando tecnologías de vanguardia y realizando demostraciones en vivo donde también se mostraron otras innovaciones como por ejemplo cámaras multisensor, dispositivos móviles de seguridad como las cámaras corporales o el terminal de control de accesos **C·CURE Go Reader.**

Johnson Controls Security Products se siente orgullosa de haber formado parte de un evento destacado como **Security Forum** y agradece su presencia a todos los asistentes que visitaron el camión de demostraciones y participaron activamente en sus demostraciones interactivas.

AXIS COMMUNICATIONS

AXIS Object Analytics ahora ofrece conteo de cruce de línea para una supervisión más efectiva

Disponible en la versión beta de la última edición de **AXIS Object Analytics**. Esta función inteligente cuenta los objetos que cruzan una línea virtual en la dirección definida y puede activar un evento siempre que el número de objetos seleccionado haya cruzado la línea. Los datos pueden consultarse de diferentes formas e integrarse en aplicaciones de terceros para visualizarlos de una forma más sencilla.

AXIS Object Analytics viene preinstalado en las cámaras de **red Axis** compatibles y aporta valor sin ningún coste añadido. Utiliza algoritmos basados en **IA** y condiciones conductuales para analizar la escena y el comportamiento espacial de los objetos que contiene y pasar por alto los eventos sin relevancia más habituales. Diseñado para la supervisión proactiva, permite a los usuarios centrarse en los objetos de interés y en los eventos que requieren su atención, además de recopilar información para tomar decisiones. Los escenarios pueden configurarse en unos pocos clics según las necesidades específicas de supervisión y es posible ejecutar varios escenarios simultáneamente. La aplicación supervisa la escena de forma inteligente para determinar si hay que activar un evento al detectarse determinados objetos.

Principales características:

- **Analítica de vídeo en local**
- **Clasificación de personas y vehículos**
- **Ejecución de varios escenarios simultáneamente**
- **Configuración flexible y sencilla**
- **Preinstalada sin coste adiciona**
- **Disponible con el firmware 11.3**

Esta solución de analítica escalable procesa y analiza el vídeo en directo en la propia cámara, lo que mejora el tiempo de procesamiento de los datos y minimiza los requisitos de ancho de banda y almacenamiento. Además, a través del sistema de gestión de eventos de la cámara, puede integrarse con **AXIS Camera Station** y todos los principales sistemas de gestión de vídeo.

+ información **aquí.**

BVMS 12.0 de Bosch

con detección fiable y anonimización de personas

BOSCH

Con la nueva superposición de privacidad basada en AI de BVMS 12.0, la "anonimización" de personas permite a las empresas mantener la seguridad, al tiempo que se protege la privacidad personal de los individuos capturados en vídeo.

La **superposición de privacidad basada en AI** elimina los datos personales de los vídeos pixelando a todas las personas sin exponer su identidad única, lo que garantiza el **cumplimiento de las leyes y normativas** de protección de datos en todo el mundo.

Al mismo tiempo, es posible identificar rasgos como el tipo o el color de la ropa, que no está inextricablemente vinculado a una sola persona. Se puede utilizar **un flujo de una sola cámara para el vídeo en directo y grabado**, permitiendo máscaras basadas en los permisos de usuario. Como ventaja añadida, los operadores pueden aplicar estas máscaras sólo para eventos específicos del sistema.

En caso necesario, los flujos de vídeo sin procesar pueden entregarse a las fuerzas de seguridad.

BVMS 12.0 es un sistema de gestión de vídeo resiliente y modular que ofrece la **máxima seguridad** gracias a su **perfecta integración** con una amplia gama de dominios y aplicaciones de seguridad, añadiendo valor en todos los puntos de contacto, desde la videovigilancia al control de accesos o la detección de intrusos.

+ información **aquí.**

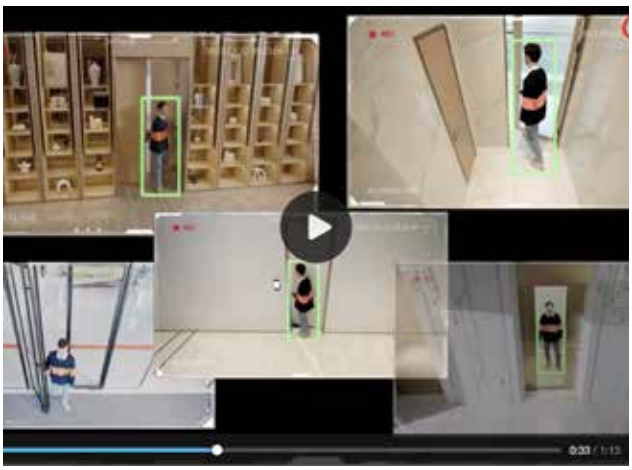
Dahua lanza una nueva tecnología AcuPick ofreciendo una búsqueda rápida y precisa

Dahua Technology ha lanzado AcuPick, una tecnología de búsqueda de video basada en IA diseñada para localizar videos objetivo de manera precisa y conveniente. El algoritmo de AcuPick integra cámaras IP y grabadores de video en red ofreciendo una búsqueda rápida, una operación sencilla y una alta precisión, lo que la convierte en un líder en avances tecnológicos dentro de la industria.

AcuPick permite a los usuarios seleccionar clips de video por objetivo en cuestión de segundos, lo cual es ideal para situaciones que requieren trazabilidad y evidencia inmediata, como el seguimiento de vándalos, de vehículos o la localización de un niño perdido en un centro comercial.

A diferencia de los métodos tradicionales, **AcuPick** filtra información innecesaria y localiza directamente los clips de video del objetivo, lo cual ahorra tiempo en la búsqueda. La función de **Búsqueda Inteligente por Intrusión** permite buscar objetivos incluso sin conocer el momento exacto de su aparición. Al seleccionar el tipo de objetivo y delinear un área de intrusión, **AcuPick** ayuda a localizar objetivos y recuperar videos de todas las ubicaciones en las que estuvo presente el objetivo.

AcuPick es una herramienta vital en diversas industrias, ya que ofrece soluciones innovadoras para superar los desafíos de búsqueda de objetivos humanos/vehiculares en entornos digitales complejos.



DESICO®

Vigiplus PSIM
enlaza con Telegram

Vigiplus PSIM añade la opción de notificar eventos a través de la aplicación de mensajería Telegram. Las notificaciones de eventos desde Vigiplus PSIM a terceros sistemas o a dispositivos móviles siempre ha sido una funcionalidad importante para mantener a los usuarios de Vigiplus conectados con los eventos que puedan suceder en una instalación.

Desde hace ya varias versiones, **Vigiplus PSIM** cuenta con esta funcionalidad a través de sms, mail o incluso a través de su propia aplicación **Vigiplus Mobile**. Gracias a la tecnología en cloud, se añade esta nueva forma de notificar eventos a través de la conocida plataforma de mensajería **Telegram.**

El proceso es tan sencillo, que basta con añadir en **Vigiplus PSIM** los correos electrónicos de las personas que desean recibir los mensajes a través de **Telegram**. Las personas que se suscriben al servicio reciben un correo a través del que se suscriben a las notificaciones. A partir de ese momento todas las notificaciones que se han configurado en **Vigiplus** para ser enviadas por **Telegram** son recibidas a través de este servicio cloud.

Además de recibir notificación de eventos, también es posible enviar mensajes por **Telegram** o enlazar con la **app Vigiplus mobile** para conocer más detalle (en caso de tenerla instalada).

+ información **aquí.**

Exivo

Simplifica y mejora tu gestión de accesos

dormakaba

exivo es la solución integral de control de acceso de dormakaba -compuesta de cerraduras, cilindros y lectores de acceso inteligentes y de funcionamiento autónomo-, que permite a las empresas de cualquier tamaño y sector controlar de manera inmediata y segura quién tiene acceso a sus instalaciones y en qué momentos.

Por ejemplo, los derechos de acceso de los visitantes para horas y salas específicas. Esto lo consigue gracias a su plataforma basada en la nube, ofreciendo así, el control total de todos los derechos de acceso, para cada estancia y persona.

Se trata de un sistema Cloud en el que destaca la sencillez a la hora de su puesta en marcha: no requiere un software especial o un servidor in situ y no interrumpe el funcionamiento al hacerlo. Esto supone un importante ahorro de costes ya que no necesita de una infraestructura de IT adicional.

Abrir puertas nunca ha sido tan fácil: simplemente comparte la llave digital en la aplicación y deja que tus usuarios entren con sus dispositivos móviles.

exivo hace que el control de acceso sea sencillo, seguro y cómodo. Ahora puedes conceder derechos de acceso sobre la marcha y utilizar tu tiempo para cosas más importantes.

exivo
está a tu disposición las 24 horas del día, estés donde estés

+ información **aquí.**

Seguridad Avanzada, Protegiendo sus instalaciones con Videovigilancia Inteligente

VIDEOSISTEMAS FFV GEUTEBRÜCK

Las cámaras PNS -PRO IA han llevado la calidad de las imágenes y las funciones inteligentes a un nivel superior. Gracias a su algoritmo avanzado, pueden detectar y clasificar con precisión personas y vehículos. Estas cámaras ofrecen funciones inteligentes y analíticas avanzadas que permiten tener una supervisión total de las instalaciones.

Algunas de ellas son:

- **Intrusión de persona:** protege áreas de amenazas e informa con alarmas ante entradas no autorizadas.
- **Merodeo:** Si hay personas y/o vehículos más tiempo del preestablecido en el área que desee proteger, lo informa con una alarma.
- **Cruce de línea:** Podrá establecer líneas de control con las cuales el sistema le informará cada vez que una persona o vehículo atraviesa las mismas.
- **Detección avanzada de movimiento:** Evita falsas alarmas al excluir movimientos irrelevantes como árboles o sombras, enfocándose en personas y vehículos en zonas específicas.
- **Conteo de personas:** Permite controlar el aforo y obtener datos valiosos para la inteligencia empresarial.

Las **cámaras IA**, junto con los **grabadores Geutebrück** facilitan el día a día del personal de seguridad, ya que proporcionan alarmas personalizadas y facilitan la búsqueda a través de filtros, permitiendo buscar por evento (intrusión, merodeo, etc.), por color de vestimenta (tanto superior e inferior) de las personas que generaron alarma, color del vehículo, etc.

+ información aquí

La conexión de puntos en el Internet de las Cosas (IoT) utilizando MQTT hace que nuestras ciudades y edificios sean más inteligentes

El protocolo MQTT (Message Queue Telemetry Transport) es un estándar para compartir mensajes entre dispositivos conectados (Internet de las Cosas o IoT). Fiable y ligero, con un consumo de ancho de banda mínimo, usa el método «publicación-suscripción»: pone en cola, comparte y transmite mensajes de forma eficiente. Basado en estándares abiertos, es flexible para trabajar con gran cantidad de dispositivos, en múltiples aplicaciones.

MQTT ha llegado a la gama completa de cámaras con **Inteligencia Artificial de Hanwha Vision** y, con ella, todos los beneficios y posibilidades que ofrece el protocolo de comunicaciones.

Así el video y los **dispositivos IoT** son fuentes de datos visuales, ambientales, de audio, de temperatura y otros tipos: reunir todos los datos en una interfaz fácil de entender, hace posible una toma de decisiones apoyada en toda la información disponible.

Como ejemplos de aplicación pueden citarse:

- **Retail:** Datos sobre ocupación y del movimiento en zonas específicas ayudará a definir niveles de dotación de personal y el uso correcto de los sistemas de climatización
- **Ciudad:** Comprender el flujo de vehículos y personas ayudará al diseño de calles y espacios urbanos, así como la definición de servicios de mantenimiento y seguridad.

El **uso de IoT** más los datos de vídeo permite ver, en tiempo real, lo que está sucediendo, y así mejorar los tiempos de respuesta y adaptar una ciudad a las necesidades de sus ciudadanos.

HID Presenta la primera tarjeta Eco Seos®

fabricadas con fuentes sustentables (Bambú) en lugar de PVC

Recientes informes de mercado, indican que la mayoría de las organizaciones clasifican el clima y la sostenibilidad como prioridades corporativas. Como resultado, están recurriendo a materiales renovables y amigables con el medio ambiente tanto como sea posible, además de disminuir el consumo de energía y residuos.

Bajo este contexto, **HID** presenta las nuevas tarjetas de acceso altamente seguras fabricadas con bambú, un recurso renovable que crece rápidamente y requiere menos agua y pesticidas que los materiales tradicionales de tarjetas. Demostrando la innovación continua de la marca sin comprometer la seguridad y la experiencia de sus clientes.

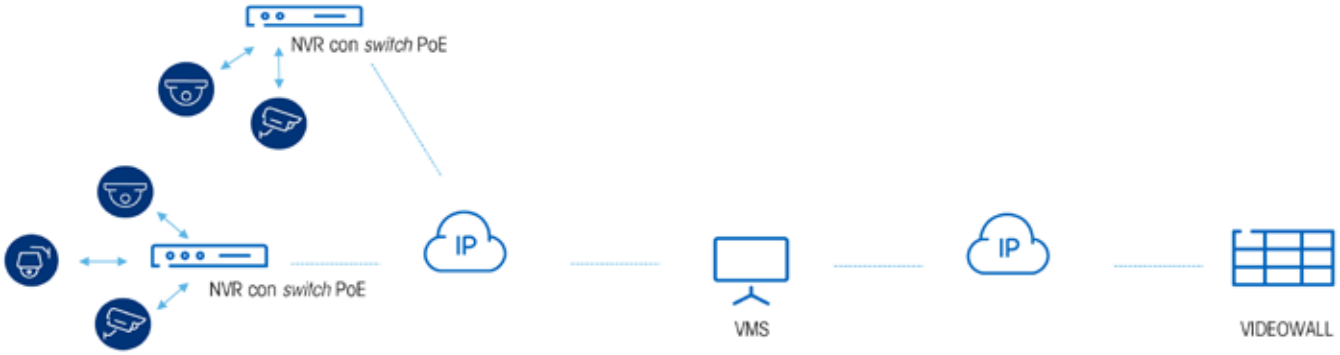
HID Eco Seos es la mejor opción sostenible dentro de los ecosistemas de acceso físico, ya que respalda una cadena de valor más respetuosa con el medio ambiente en entornos donde todavía se requieren tarjetas de acceso físicas.

Las **tarjetas HID Eco Seos de bambú** también respaldan a las organizaciones que buscan certificaciones de sostenibilidad, como las internacionalmente reconocidas certificaciones **LEED (Liderazgo en Energía y Diseño Ambiental), la BREEAM (Certificado de Construcción Sostenible)** y **la certificación Cero Residuos a Vertederos (Zero Waste to Landfill).**

+ información sobre las **nuevas tarjetas Seos Bambú aquí.**

Infraestructura de videovigilancia cibersegura

Gracias al switch PoE, el videograbador detecta un posible sabotaje por sustitición dispositivo.



Los videograbadores de Lanaccess pueden integrar hasta 28 conectores PoE.

LANACCESS
Discover the power of video.

Claves para un videograbador ciberseguro

En esta nota informativa, abordamos las características de un videograbador ciberseguro por diseño.

En primer lugar, es r**ecomendable que el sistema operativo sea diferente a Windows**, el objetivo principal de los ciberdelincuentes. Los videograbadores que no corren en Windows, no son susceptibles a los ataques más comunes.

Los protocolos que usen los videograbadores deben estar encriptados (HTTPS, FTPS y SSH), y establecer un cifrado de la comunicación entre la cámara y el equipo. Además, el propio equipo debe bloquear temporalmente el acceso a cualquier usuario que haya intentado iniciar sesión repetidas veces.

Por otro lado, **los videograbadores deben estar diseñados para prevenir ataques DDoS**, que buscan saturar el sistema con solicitudes ilegítimas. Deben detectar ataques de forma automática y tener la capacidad para bloquear la dirección MAC del atacante.

No menos importante, los **NVR** deben tener las funciones propias de un firewall, y se deben habilitar solo los puertos necesarios. También deben estar protegidos contra la carga de versiones falsas de firmware.

Por último, es recomendable usar videograbadores con switch PoE integrado en el propio equipo, y que este switch permita el control avanzado de los dispositivos IP.

"Lanaccess fabrica videograbadores ciberseguros por diseño en todas estas áreas"

Locken se convierte en ISEO Ibérica Systems & Services

ISEO®
ULTIMATE ACCESS TECHNOLOGIES

"Together is the Key"

Los cambios realizados tienen como objetivo lograr una única entidad bajo la marca

ISEO Ultimate Access Technologies

armonizando la marca y maximizando la difusión de la oferta completa de la compañía.

Asimismo, se busca integrar el modelo de negocio de Sistemas y Servicios (por el cual Locken es reconocido), como parte integral de la oferta de ISEO a nivel mundial y como un pilar clave en la actual y futura estrategias del grupo.

Se espera que estos cambios faciliten la optimización de los procesos, impulsen las sinergias de trabajo y permitan la consecución de los ambiciosos objetivos de crecimiento comunes.

Sicuralia

Vallado sensor HSF Activa®

Máxima capacidad de detección, libre de falsas alarmas.

HSF Activa® es un vallado de seguridad compuesto por paneles de mallas rectangulares electro soldados, donde los postes tienen integrado en el interior un sensor de vibración piezoeléctrico invisible, que proporciona una señal de alarma individual para cada segmento de vallado.

Su malla especial anti-escalada con celdas de 76,2 x 12,7 mm dificulta y ralentiza el escalado.

Este sistema de detección perimetral está integrado dentro de la valla, siendo totalmente invisible.

La detección consiste en un sensor de vibración piezoeléctrico (o MEMs) invisible con capacidad de detección por vibración y corte. El bus de comunicaciones discurre por el interior del vallado y está protegido contra agresiones externas.

El sistema puede estar equipado con una banda sensora opcional en la parte superior que permite detectar el franqueamiento superior de la valla.

En el corazón de **HSF Activa®** hay un sofisticado sistema de detección Pin-Point (+/- 2.5m de resolución de detección) hecho de **Sensores de Detección Oculta (HDS)** que incluyen un sensor piezoeléctrico con microprocesador que procesa la señal generada por las vibraciones mecánicas aplicadas a la valla

HSF Activa® dispone también de su propia plataforma de monitorización y gestión de alarmas, **HyperPower**, gracias a la cual puede integrarse en cualquier VMS o PSIM de terceros, tales como **Qognify QVMS®, Desico, Milestone, Citel, Arteco, Genetec, Geutebruck, BACNet, Honeywell, Siemens, Tyco, Jhonson Controls, Alesys, Thales, Cortech,** entre otros.

+ información **aquí.**

CIBERSEGURIDAD Y LEGISLACIÓN

Manuel
Carpio

VOCAL DEL FORO NACIONAL
DE CIBERSEGURIDAD
DIRECTOR DE SEGURIDAD
EN ARMATUM360

LA CIBERSEGURIDAD ES UN INGREDIENTE BÁSICO EN EL PROCESO DE DIGITALIZACIÓN DE NUESTRA SOCIEDAD Y EN LA CREACIÓN DE UN ENTORNO ECONÓMICO QUE ATRAIGA INVERSIÓN Y QUE IMPULSE EL CRECIMIENTO ECONÓMICO. ESTAS SON DOS DE LAS SEIS PRIORIDADES DE LA COMISIÓN EUROPEA DURANTE SU ACTUAL MANDATO.

El fin de año 2022 vino acompañado de fuegos artificiales legislativos desde la Comisión en materia de ciberseguridad. Así, el pasado 27 de diciembre de 2022 el Diario Oficial de la Unión publicó, de una sola tacada, el texto final de la **Directiva sobre seguridad en redes y en sistemas de información (NIS2)**, la **Regulación sobre resiliencia operacional digital (DORA)** y **la relativa a la resiliencia de las entidades críticas (CER).**

Además, el Parlamento Europeo y el Consejo venía revisando una propuesta de la Comisión de Regulación sobre Ciberresiliencia, **"The Cyber Resilience Act" (CRA)**, un nuevo marco de requisitos para mejorar la seguridad del hardware y software que usamos y consumimos, incluyendo todo un esquema de certificación. Todas estas nuevas normas desembocarán en reglamentos nacionales y europeos cuyo cumplimiento será obligatorio dentro de aproximadamente dos años.

Pero también a nivel nacional, unos meses antes, el Boletín Oficial del Estado del 4 de mayo de 2022, publicaba el nuevo Esquema Nacional de Seguridad (ENS). Esta actualización del ENS ha perseguido, en primer lugar, alinear el instrumento con la transformación digital del sector público y sus proveedores del sector privado. En segundo lugar, ha introducido la capacidad de ajustar los requisitos del ENS a necesidades específicas de determinados colectivos de entidades, o de determinados ámbitos tecnológicos, dando respuesta a las nuevas demandas.

Como se ve, si bien otras potencias mundiales son innovadoras en sectores económicos clave como el **5G**, o la **IA**, la Unión Europea es un gran innovador y exportador regulatorio. Hay quien se consuela pensando que somos fuente de inspiración para otros países, como ya ha ocurrido anteriormente en lo relativo al tratamiento de datos de carácter personal.

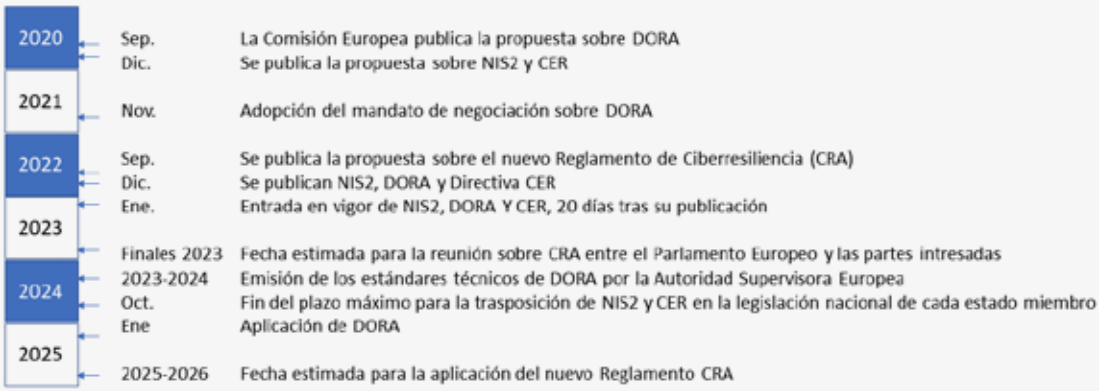
Frente a las regulaciones que tienen carácter de Directiva, debemos tener en cuenta que **DORA** es un reglamento, lo que implica aplicación directa y sin interpretaciones de los Estados miembros, es sectorial, y tiene un alcance más amplio que las Directivas que la acompañaron. Se trata de una normativa orientada a la gestión de riesgos en los negocios que introducirá un conjunto completo de reglas para que las empresas del sector financiero fortalezcan su 'resiliencia operativa digital' y puedan prevenir y mitigar las ciberamenazas. Cabe señalar que, al otro lado del Atlántico el **Departamento de Servicios Financieros de Nueva York (NYDFS)** está desarrollando otra regulación similar.

Estas cinco regulaciones están llenas de interrelaciones y solapes. Por no extendernos en exceso, nos ceñiremos en este artículo a las que nos vienen de Bruselas. Pese a que uno de los objetivos marcados por la Comisión Europea era disponer de un marco regulatorio europeo menos complejo, es posible que, la irrupción simultánea de **NIS2, DORA** y **CER**, venga acompañada de incertidumbre en algunas organizaciones por los posibles solapamientos o priorización en la aplicación de las exigencias establecidas por cada uno de ellos. Un ejemplo de este solapamiento se manifiesta en que **NIS2** mantiene dentro de su alcance a las entidades financieras y aseguradoras que, al mismo tiempo, se encuentran bajo las obligaciones de **DORA.** Sin embargo, aunque estas han de cumplir ambas regulaciones, **NIS2** deja muy claro que, cuando se trate de entidades de crédito, deben aplicarse las disposiciones de **DORA** en relación al riesgo tecnológico, así como en la notificación de incidentes, las pruebas de resiliencia, el intercambio de información y los riesgos de proveedores tecnológicos.

Otra área de solape es el intercambio de información y la cooperación entre las autoridades competentes, tanto las designadas bajo **DORA** por un lado, como las figuras y autoridades competentes establecidas con arreglo a **NIS2** por otro. En cuanto a la **Directiva sobre Resiliencia de las Entidades Críticas (CER)** que, de

forma similar a **NIS2**, pretende alcanzar un marco de ciberseguridad común en la UE para la protección de las organizaciones pertenecientes a sectores críticos, marca la diferencia centrándose más en la resiliencia física de las organizaciones que en la resiliencia digital, contemplando en su espectro de amenazas, entre otras, ataques físicos o desastres naturales.

Adicionalmente, ya ha sido publicado el borrador del nuevo **Reglamento de Ciberresiliencia (CRA)** que, a priori, complementará a **NIS2** poniendo el foco en la seguridad de los productos y servicios digitales durante sus fases de desarrollo y distribución. Por tanto, su cumplimiento permitirá a los proveedores de dichos productos estar más alineados con los requisitos de seguridad que **NIS2** exige a la cadena de suministro de las entidades esenciales e importantes. No obstante, habrá que esperar a su publicación oficial para determinar el grado de impacto que tendrá sobre las organizaciones.



Calendario legislativo "ciber" europeo.

La Directiva NIS2

Uno de los puntos más destacables de la **nueva Directiva NIS2** es que ninguna organización, que por su naturaleza sea considerada entidad esencial o crítica, será notificada de que se encuentra bajo el alcance de **NIS2** por la autoridad competente, al menos de momento y a la espera de la transposición. Recae por completo en las organizaciones la responsabilidad de autoidentificarse como entidad esencial o importante, de acuerdo a los criterios establecidos en la nueva Directiva. Para **NIS2**, una entidad que, perteneciendo a un sector importante dispone de una gran cuota de mercado, podría considerarse esencial debido a su tamaño, por lo que dicha autoevaluación no va a estar exenta de polémica.

Otro asunto candente es la debida atención a la seguridad de la cadena de suministro; las organizaciones tendrán que implementar políticas y procedimientos que permitan evaluar la aplicación de medidas adecuadas de ciberseguridad en todos sus proveedores de servicios y productos TIC. Además, deberán revisar sus actuales cláusulas y exigencias contractuales para garantizar el cumplimiento de **NIS2**.

Las organizaciones deberán asignar responsabilidades en miembros de la alta dirección, que vendrán acompañadas de la exigencia de invertir, con carácter periódico, en su concienciación y formación en materia de ciberseguridad. Así se espera garantizar que disponen de las capacidades necesarias para la identificación de riesgos y la evaluación de las medidas de ciberseguridad implementadas en la organización que dirigen y por las que deberán responder en caso de producirse infracciones en el cumplimiento de sus obligaciones.

Ley de Resiliencia Cibernética o Ciberresiliencia

Este borrador sigue su camino, pendiente de acordar una posición común en varios puntos donde hay rozamiento. Su objetivo es evitar que se comercialice en la Unión Europea dispositivo alguno que no respete los requisitos de ciberseguridad establecidos cuando se conectan a redes telemáticas. Se excluyen algunos, como los desarrollados exclusivamente para el ámbito de Defensa, y se encuentran en debate los que tienen uso dual.

Sorprende que sea posible que muchos productos sigan siendo comercializados a sabiendas de que contienen vulnerabilidades. El motivo es que los fabricantes carecen de incentivos para invertir en el diseño y desarrollo seguro de los productos y proporcionar actualizaciones de seguridad. Primero, porque el coste de los incidentes lo asumen principalmente los usuarios, ya sean operadores de servicios esenciales o simples consumidores. En segundo lugar, porque los usuarios, a menudo no solo carecen del conocimiento necesario para valorar la ciberseguridad de un producto, sino que incluso desconocen los riesgos de seguridad asociados. Finalmente, los fabricantes suelen intentar introducir nuevos productos en el mercado lo más rápido posible, priorizando el desarrollo de funciones y la compatibilidad con los productos existentes.

La Comisión considera esta situación como un fallo estructural del mercado, y por eso adoptó la propuesta de **Ley de Ciberresiliencia**. Cuando entre en vigor, tras su negociación por el Parlamento Europeo y el Consejo, los fabricantes de productos con elementos digitales deberán implementar requisitos de seguridad, someterse a una evaluación de conformidad y colocar la marca "CE" antes de ser comercializados en el mercado europeo.

Con ello se pretende reducir el número de vulnerabilidades y, por tanto, de ciberataques. En principio aplicará a todos los productos conectados directa o indirectamente a otro dispositivo o red: tanto el hardware y componentes comercializados separadamente (ordenadores, teléfonos móviles, equipamiento de red, etc.), como el software y componentes comercializados aparte (sistemas operativos, aplicaciones, videojuegos, etc.). Quedan fuera de su aplicación el software como servicio **(SaaS)** y el software libre y de código abierto desarrollado al margen de una actividad comercial.

La legislación se ha diseñado para cubrir toda la cadena de suministro. Por ejemplo, los teléfonos inteligentes se incluirían en el ámbito de la regulación y deben por tanto respetar los requisitos de ciberseguridad y adherir el marcado **"CE"**.

El fabricante del teléfono deberá por tanto comprobar el marcado **"CE"** adherido a los componentes hardware y firmware y, si es el caso, al sistema operativo. Por tanto, los consumidores y usuarios comerciales podrán confiar en el marcado **"CE"** del producto como un indicador de que, no solo el producto final sino también todo el hardware y componentes de software dentro de dicho producto han sido desarrollados tomando en serio la ciberseguridad.

El reglamento DORA

El **Reglamento de Resiliencia Operativa Digital**, es conocido por el nombre de **DORA** y nace para regular la forma en que las entidades financieras gestionan el riesgo digital en las finanzas, en un entorno de transformación digital, nuevos participantes y grandes organizaciones tecnológicas.

Respecto a su alcance e implicaciones, y a grandes rasgos, **DORA** impacta en las instituciones de la siguiente forma:

- **La gestión del riesgo TIC, propio y de terceros proveedores.**
- **Los incidentes y las notificaciones de incidentes relacionados con las TIC.**
- **Las pruebas de resiliencia operativa digital, que comprendan una variedad de evaluaciones, pruebas, metodologías, prácticas y herramientas.**
- **El intercambio de información entre entidades financieras.**
- **La monitorización continua del funcionamiento de los sistemas y herramientas.**

DORA considera y actualiza los requisitos de riesgo de las tecnologías de la información y la comunicación en todo el sector financiero de la UE de forma homogénea, para que sea capaz de mantener operaciones resilientes en caso de una grave interrupción operativa y recuperarse de ellas.

Las organizaciones financieras de la UE deberán seguir un enfoque basado en el riesgo para establecer una sólida gestión de la red y de la infraestructura y utilizar mecanismos automatizados para aislar los activos de información afectados en caso de ciberataques.

La **propuesta de reglamento DORA** señala que las entidades financieras identificarán todas las cuentas de sus sistemas TIC, los recursos de red y los equipos de hardware, y mapearán los equipos físicos considerados críticos. El diseño de la infraestructura de red deberá garantizar su compartimentación y permitir su corte instantáneo con el fin de minimizar y prevenir el contagio, especialmente en el caso de los procesos financieros interconectados.

Además de la gestión uniforme de los riesgos de las TIC, las organizaciones de servicios financieros de Europa deberán informar a las autoridades competentes de todos los incidentes importantes relacionados con las TIC.

La ley impactará en las organizaciones proveedoras de empresas de servicios financieros. Establece que algunos de los proveedores TIC serán designados como críticos y aquí es donde radica una de las principales novedades: en el establecimiento de un marco especifico de supervisión para ellos. Estos serán supervisados por la UE, respondiendo a la petición de información, documentación cuando sea necesaria. En caso de incidente de ciberseguridad, serán los proveedores los que deban prestar asistencia a las organizaciones sin coste adicional

A pesar de su alcance intencionalmente amplio, **DORA** introduce algunos elementos de proporcionalidad, es decir, las entidades financieras incluidas en el alcance deberán cumplir con **DORA** teniendo en cuenta su tamaño y perfil de riesgo general, así como la naturaleza, escala y complejidad de sus servicios, actividades y operaciones, entre otras variables, pudiendo aplicar también a PYMES.

La Directiva CER

La **nueva Directiva CER** sustituye a la **Directiva Europea de Infraestructuras Críticas de 2008** con el fin de fortalecer la resiliencia de la infraestructura crítica frente a amenazas de la naturaleza, ataques terroristas, amenazas deliberadas internas o sabotajes. Con este fin, tiene en cuenta la existencia de un panorama dinámico de amenazas, entre las que figuran las híbridas y terroristas en evolución y a los fenómenos meteorológicos extremos.

Aunque la Directiva original solo se refería expresamente a los sectores de la Energía y del Transporte, su transposición al ordenamiento jurídico español amplió su aplicación a los 12 sectores estratégicos ya conocidos, y creando el Sistema PIC bajo la dirección del Ministerio del Interior, a través del **Centro Nacional de Protección de Infraestructuras Críticas (CNPIC).**

En su revisión de 2019, se planteó la necesidad de modificar el enfoque para garantizar que se tuvieran en cuenta los riesgos derivados de una mayor interconexión y carácter transfronterizo de las operaciones que utilizan infraestructuras críticas. Las medidas de protección relativas únicamente a activos aislados no bastaban para evitar todas las amenazas.

Sin embargo, la transposición de la **Directiva NIS** malogró el concepto de integralidad de la seguridad de las infraestructuras críticas, separando conceptualmente del sistema PIC la protección de los servicios esenciales que emanan de estas, con el pretexto de propugnar medidas para garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

Aunque la **Directiva PIC** ofrecía notables lagunas, también la Directiva NIS nació con atronadores silencios, como el relativo a los requerimientos de seguridad para los dispositivos, que ahora se pretende parchear mediante la Ley de Resiliencia Cibernética.

Como se ha visto, simultáneamente a la **Directiva CER** se promulga la **Directiva NIS2**, y se hace necesario buscar la coherencia entre ambas normas, según se había denunciado repetidamente. Respondiendo a esta necesidad, se excluye del ámbito de aplicación de la **Directiva CER** las materias reguladas en la **NIS 2**, con la intención de salvaguardar la especialidad de las normas. No obstante, serán los Estados Miembros los que, en función de la madurez de sus respectivos modelos de seguridad, deberán transponer ambas directivas en la forma que mejor contribuya a potenciar dichos modelos. Esa es la estrategia de la **Directiva CER**, que exige a los Estados un enfoque global de la resiliencia de las entidades críticas.

El advenimiento de esta hemorragia legislativa debería convertirse en una doble oportunidad para España. En primer lugar, una oportunidad para integrarla bajo una misma y única regulación nacional, ahorrando costes de todo tipo al erario público y unificando el mando para hacer frente a los ataques ciber. En segundo lugar, debería ser una oportunidad para desarrollar e impulsar a la industria y los servicios de seguridad españoles.

CONOCE A UN

SOCIO

Pedro de Ibarrondo

SOCIO Nº 125

pedro.ibarrondo@securitycloudservices.es

Buenos días Pedro. Lo primero que te pido es que te presentes al resto de socios para que podamos conocerte.

Mi nombre es Pedro de Ibarrondo, padre de dos hijos y abuelo de 6 nietos a los que considero mi más alta prioridad en el terreno personal. Vine a vivir a Madrid procedente de Bilbao a los 6 años, pero mantengo unas profundas raíces en Bilbao con familiares y amigos "de pantalón corto" que valoro enormemente.

Profesionalmente, después de mis estudios en USA regresé a Madrid y comencé en 1978 mi primer trabajo en **ADEMCO** y he mantenido desde entonces Madrid como base de mis actividades durante el resto de mi vida, bastante viajera, donde me encuentro muy cómodo e integrado, con mi familia.

¿Cuál es tu formación académica?, Con tu titulación como Ingeniero técnico, ampliaste tu formación en Estados Unidos ¿Cómo fueron aquellas experiencias?

Complete mi titulación de Ingeniero técnico Industrial. Rama Electrónica en Junio de 1975 en la Universidad Politécnica de Madrid, y tuve la oportunidad de completar mi educación en EEUU al ser admitido en 1976 en el **Programa de MSEE Master of Science in Electronic Engineering** en Northrop University- Inglewood Ca. USA, donde hice una especialización **"Major in Semiconductor Devices & Microwaves"** en Junio 1977. Añadiendo una opción de Gestion para ingenieros: **"MSEMO Master of Science in Engineering-Management Option"**, durante los últimos 6 meses, acabando ambas titulaciones en octubre de 1977, y regresando a España para mi primer trabajo, con **ADEMCO** casi de manera inmediata.

¿En qué empresas has desarrollado tu actividad profesional?

Después de completar mis estudios en la Univesidad de Northrop en Los Angeles-California, comienza mi andadura profesional en 1978 en España como representante de **Ademco** –el mayor fabricante a nivel mundial de Equipos de Seguridad en ese momento– con el encargo de homologar en **Telefónica de España** los primeros equipos de Comunicación Digital que se homologaron en España en 1978, comenzando a desarrollar el mercado de Monitorización que se iniciaba en ese momento en España través de Distribuidores y posteriormente formando en enero 1980 **Ademco-Sontrix España, S.A.** como Consejero-asociado y Director, iniciando la andadura como Fabricante-Distribuidor en ese mismo 1978, pasando a ser Director General en 1984 para España y Portugal.

En 1999 tomo responsabilidad internacional llevando el Sur de Europa como Presidente-Consejero Delegado de **Ademco International** en España e Italia, que más tarde a final de 1999 pasaría a formar parte del **Grupo Honeywell**, que adquirió **Pityway Corporation**, siendo entonces responsable de **Honeywell Security Southern Europe**, que más tarde segrega la parte de fabricante como **Honewell Security** y la de Distribuidor, creando la nueva marca de distribución **ADEMCO-Distribucion-ADI** de la que me hacen responsable para Sur de Europa, posteriormente con la marca **ADI-Internacional** como Distribuidor Muiti marca tratando con los principales fabricantes del sector además de las del **grupo Honeywell.**

En febrero 2005 fui nombrado **Honeywell National Executive** para España & Portugal para todas las divisiones del grupo y miembro de la **American Business Council –ABC–** como representante de Honeywell España.

En diciembre 2009, y tras la salida de **Honeywell** a la terminación de mi contrato, me establezco como Consultor Independiente trabajando en una importante adquisición que se completa en dic 2019, la adquisición de **Tecniserv** por parte de **Securitas Alert Services - BE**, pasando a mi primera experiencia en el sector de las Centrales receptoras de Alarma y Servicios de Seguridad como Consejero-Director General de **Tecniserv - Securitas Alert Services del Grupo S ecuritas- BE** en España hasta 2012 que se convirtió en la **CRA-SECURITAS ALERT SERVICES** en España, pasando más tarde a formar parte de Seguritas Seguridad España S.A.

Como consultor independiente, en febrero de 2010 soy nombrado Consejero Independiente del **Grupo Azkoyen**, del que soy nombrado miembro del Comité de Auditoría, y su secretario desde febrero de 2015 hasta mayo de 2016.

Al conocer más en profundidad el mundo de las CRAs de primera mano, comprendí la necesidad de las CRA-PYMES de racionalizar las inversiones necesarias en Tecnología & Servicios para poder ser capaces de sobrevivir y de competir con las grandes CRAs del mercado. Capacitándolas para ser capaces de ofrecer servicios de manera fácilmente accesible también para aquellos Instaladores Independientes–Dealers que sirven a sus clientes finales, de manera que sean capaces de ofrecer Servicios especializados de CRA para sus clientes con los últimos avances del mercado.

En julio 2012 me estreno como empresario con **Security Cloud Services S.L. –SCS-** creando esta nueva empresa de la que soy CEO, como proveedor de Infraestructura & Comunicaciones de Servicios Centralizados de Seguridad en CLOUD fundamentalmente para Centrales Receptoras de Alarma, pionera de este tipo de servicios en Cloud en nuestro sector. La Infraestructura y Comunicaciones en Cloud que ofrece SCS aloja tanto las BBDD de los programas de gestión de estas CRAs en estrecha colaboración con IBS –proveedor del programa de gestión de alarmas– que aloja las BBDD de las diferentes receptoras que se van alojando en SCS.

La propuesta de SCS es especialmente eficaz en aquellas CRAs de nueva creación que parten de su establecimiento con la Infraestructura y BBDD en SCS, con un ahorro de puesta en marcha del 75% de la inversión inicial, muchas de ellas operando en "Modelo Colaborativo" con CRAs-Master especialistas, que a su vez crecen con este modelo de desarrollo de negocio que, además, ayuda a revitalizar el mercado de los instaladores y mantenedores independientes.

También soy un gran convencido de la asociación en el sector, y tengo el orgullo de ser uno de los miembros fundadores de **AES- Asociación de Empresas de Seguridad** –y del comité ejecutivo desde su creación hasta 2010, representando a **AES**– junto con el Presidente **Antonio Ávila en Euralarm**: European Industry association desde 1996 hasta 2007. Miembro activo actualmente de los GT de Ciberseguridad & Centrales Receptoras de Alarma.

Tras más de 30 años en el sector de la distribución de productos de seguridad, pasaste al mundo de las centrales receptoras de alarma ¿Qué supuso para ti este cambio?

Como decía un buen amigo mío del sector, es ver el mismo mercado, "pero desde el otro lado de la barra...". Realmente las CRAs e Instaladores Independientes eran la base de mis clientes de toda la vida, pero desde "el otro lado de la barra..." te das cuenta de lo difícil que es rentabilizar una CRA, escoger las inversiones –para amortizarlas razonablemente– en los productos adecuados para mantener al día los servicios prestados por la CRA considerando la importante evolución de los productos en los últimos años ,con el nivel de inversión necesario para satisfacer a todos tus clientes.

Como gestor de la plataforma independiente SCS debo de ser " Agnóstico " respecto a fabricantes y los diferentes proveedores del sector , con los que siempre he mantenido una buena relación, ayudando con mi experiencia como Distribuidor multi-marca en ADI –Internacional.

Veo que tu interés por el mundo de las CRA te llevó a crear SCS. De forma somera ¿qué innovaciones ves en ese sector y como imaginas su futuro?

La creación de este **Servicio Centralizado de Seguridad –SCS –** como **Servicio en CLOUD pionero en España** fue un paso muy importante en mi vida profesional como empresario.

En mi opinión se han introducido mejoras y avances más importantes en los últimos 5 años que en los 30 años anteriores, tanto a nivel de fabricantes, inicialmente de Video que tuvo su explosión , como de fabricantes de Intrusión, aportando importantes innovaciones, incorporado imágenes asociadas a una alarma, el inicio de la Video-verificación y más tarde clips de video apoyadas en las importante mejoras tecnológicas del mundo IOT, y desarrollo de la comunicaciones, que han impulsado y posibilitado innovaciones tecnológicas muy importantes basadas en servicios Cloud prestadas por los nuevos fabricantes. La impresionante evolución del mercado de video y su volumen posibilita la reducción de costes y la accesibilidad al cliente final.

Estas nuevas tecnologías y el desarrollo de IOT ha generado nuevas soluciones y servicios en Cloud –propios, ofrecidas por los nuevos fabricantes más innovadores que han posibilitado el desarrollo de Sistemas de Gestión de video y sistemas de video-verificación, pero que requieren de una integración con los diferentes sistemas de gestión de alarmas , así como la integración con servicios de almacenamiento en Cloud que están desarrollando nuevas necesidades para el mercado, que es cada vez más complejo y necesita de herramientas para simplificar tanto el acceso como la gestión de todas estas nuevas prestaciones.

La experiencia de la evolución experimentada en el sector en estos últimos 11 años desde que se inician los servicios Cloud ha sido muy reveladora, ya que ha evidenciado la necesidad tanto de las CRAs como de sus clientes –Instaladores Independientes y clientes finales– de conectar con nuevos fabricantes que ofrecen soluciones de última tecnología conectadas a sus propias soluciones Cloud tanto para la necesaria alta y gestión bidireccional de sus instalaciones como para la Video-verificación integrada.

El futuro inmediato en mi opinión está íntimamente relacionado con la adaptación , en primer lugar a Grado-2 para diciembre de 2023, seguida de las nuevas regulaciones ya conocidas de ámbito EU como la EN-50518 y su posible incorporación al nuevo reglamento, así como la ya existente certificación del Esquema Nacional de Seguridad que será requerida para los proveedores de soluciones y servicios a la administración pública o forman parte de la cadena de suministro de dichas soluciones y servicios, y por lo tanto se encuentran dentro del ámbito de aplicación, y que muy posiblemente se extienda al ámbito de la seguridad privada, como factor diferenciador de calidad en el proceso de selección de concursos privados de grandes corporaciones en el ámbito privado.

Volviendo a los aspectos formativos ¿Qué carencias has detectado en tu relación con los ingenieros dedicados a la seguridad?

La formación, y accesibilidad de todo tipo de documentación ha mejorado de manera espectacular con las nuevas tecnologías, y los sistemas de gestión remota de todos los fabricantes han cambiado la forma de trabajar de todos nosotros, siendo el mayor problema para las empresas y los ingenieros de Sistemas de seguridad, la priorización de la formación y la efectividad del tiempo dedicado a la formación, en un entorno dedicado a las urgencias permanentes.

La clásica elección entre lo importante vs lo urgente
La necesaria adecuación de los antiguos sistemas a las nuevas tecnologías exigidas por Grado 2 men-

cionada anteriormente va a necesitar la elección de los nuevos productos y la consiguiente formación necesaria de técnicos de campo y de Operadores de CRAs, que deberán ser impartidas por ingenieros convenientemente formados para este propósito.

Va a ser necesaria la adecuación del personal técnico de las empresas de Sistemas de Seguridad- tanto Instaladoras & Mantenedoras como CRAs para asumir los nuevos Sistemas, que va a forzar a adecuar la necesaria adaptación tecnológica de nuestro sector en términos de adecuación de procedimientos – condicionados por la Ciberseguridad- absolutamente clave en este cambio tecnológico de servicios y operativa a través de Sistemas en Cloud – en el que la formación de los técnicos, con especial énfasis de la PYMES, para sobrevivir y ser capaces de competir en este entorno tan evolutivo.

Sé que los asuntos laborales absorben gran parte de tiempo, pero espero que te quede algo para dedicarlo a tus aficiones "extralaborales". ¿Cuáles son tus hobbies?

Estoy muy orgulloso de mantener amigos de los que me puedo preciar dentro de nuestro mundo de la seguridad -además de los personales como decía "de pantalón corto" – que considero muy importante en mi vida personal, pero para mí, personalmente, sobre todo la familia está por encima de todo, tengo la mayor parte de mi tiempo libre ocupado, pero sigo manteniendo reuniones con diferentes grupos de compañeros de trabajo que disfruto enormemente.

De deportes: Golf para sufrir, andar y pasear para disfrutar y la Pesca cuando puedo, a poder ser con buena compañía.

¿Qué viste en AEINSE para hacerte socio?

Siempre vimos en nuestras conversaciones entre los técnicos la falta de valoración de nuestra carrera como ingenieros dentro de nuestro sector, al ser la parte de Sistemas no tan valorada como debería respecto a otras áreas de más facturación en las grandes empresas especialmente. Creo que esto está ahora cambiando, en los últimos 5 años ha habido más avance tecnológico de sistemas que en los últimos 30 años, como dije antes. La necesidad en las PYMES es si cabe más acuciante y deberíamos desde las asociaciones hacer un esfuerzo en este sentido, dirigido a este segmento.

Negar que mi amistad desde 1978 con Alfonso Bilbao (creo que mi primer contacto profesional, era uno de mis dos Distribuidores iniciales de ADEMCO en España y testigo de mis inicios en este sector), y con otros miembros de la junta – Pedro de la Hoz, Pedro Carpintero - y varios más tuvo su peso; me convencieron sin problemas para unirme. Me siento muy cómodo en AEINSE , y trataré de colaborar más estrechamente con nuestra asociación.

¿Crees que podrías colaborar en alguno de los grupos de trabajo de la Asociación?

Espero colaborar en lo posible. Contad conmigo para lo que haga falta, aunque actualmente tengo concentrados mis esfuerzos en los dos GT de AES mencionados anteriormente; Ciberseguridad & CRAs , pero que son compatibles con AEINSE absolutamente.

¿Qué sugerencias puedes hacer a AEINSE que nos ayude a mejorar y aportar más valor a los socios?

Creo que crear grupos de información- Formación y transmisión de las nuevas tecnologías con los fabricantes actuales es una gran idea y espero colaborar en un futuro próximo con AEINSE organizando una sesión informativa de Soluciones en Cloud con fabricantes & distribuidores clave que aporten las soluciones más novedosas posibles a nuestros miembros de AEINSE.

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

JUNIO
07

ACTUALIZACIÓN LEGISLACION SEGURIDAD PRIVADA

Con fecha 7 de junio se han incorporado modificaciones en el **Real Decreto 2487/1998 de 20 de noviembre**, por el que se regula la acreditación de la aptitud psicofísica necesaria para tener y usar armas y para prestar servicios de seguridad privada.

El **Código de Seguridad Privada** –que incluye toda la legislación nacional hasta la fecha– puede descargarse **aquí.**

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

ESQUEMA NACIONAL DE SEGURIDAD (ENS)

La **Agencia Estatal Boletín Oficial del Estado** ha publicado el pasado 3 de mayo el **Real Decreto 311/2022** por el que se regula el Esquema Nacional de Seguridad. Según figura en su artículo 1:

1. Este real decreto tiene por objeto regular el **Esquema Nacional de Seguridad** (en adelante, **ENS**), establecido en el **artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.**

2. El **ENS** está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

3. Lo dispuesto en este real decreto, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la **Ley 36/2015, de 28 de septiembre**, de Seguridad Nacional.

+ INFORME COMPLETO

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

agencia española protección datos

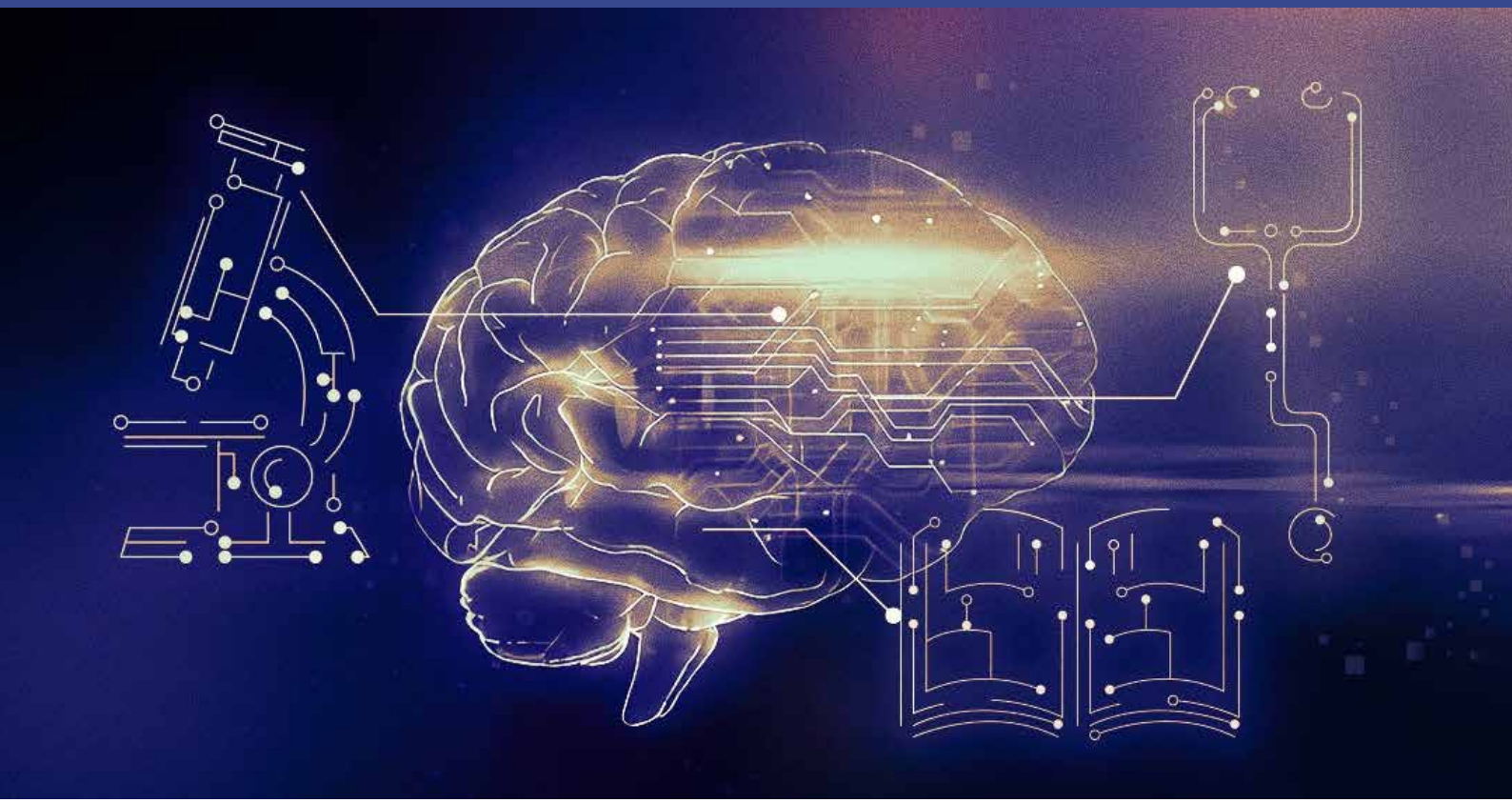
El **Boletín Oficial del Estado (BOE)** de fecha **9 de mayo de 2023**, ha publicado la **Ley 11/2023, de 8 de mayo**, de trasposición de Directivas de la Unión Europea en diferentes materias. Entre ellas una modificación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales **(LOPDGDD).**

Las modificaciones afectan fundamentalmente a asuntos relacionados con el procedimiento sancionador, las actuaciones de investigación y la presentación de reclamaciones.

En este **enlace** puede obtenerse el **texto completo de la Ley**. La parte relacionada con la **LOPDGDD** se encuentra en la Disposición Adicional Novena, página 14 del documento.

GatesNotes THE BLOG OF BILL GATES

La era de la Inteligencia artificial ha comenzado...



Artículo de **Bill Gates** sobre la **IA** en el que manifiesta su punto de vista acerca de las posibilidades presentes y futuras de la misma para reducir algunas desigualdades del mundo.

Parte de la definición de IA para, pasando por la mejora de la productividad, intuir su influencia positiva en el terreno de la salud y la educación, como ejemplos.

Finalizando con el análisis de los riesgos y problemas que puede traer consigo y aconsejando principios éticos para su uso y desarrollo.

Leer el artículo completo **aquí**

SEGURITECNIA

Seguritecnia ha publicado en el número 500 de la revista el estudio sectorial "Seguridad Privada en España: hacia 2030"

A través de una encuesta en la que han participado cerca de **500 profesionales**, realiza un análisis acerca de la evolución del sector desde ahora hasta el año 2030.

La encuesta ha consistido en **10 preguntas** que aborda los siguientes temas: tecnología, amenazas y riesgos, colaboración público-privada, normativa, recursos humanos, formación profesional, el mercado y soluciones de seguridad.

Como podía esperarse, el factor que se estima más determinante es la aplicación de la tecnología.

Descubre el resto de factores en **aquí**

LEÍDO EN...

El Confidencial
EL DIARIO DE LOS LECTORES INFLUYENTES

Economía ■ *La mano visible*

La mano visible
Por **Jesús Fernández-Villaverde**
Gráficos: Unidad de Datos

La inteligencia artificial y el futuro del crecimiento económico

En mi entrada anterior describí las ideas básicas de la inteligencia artificial. Hoy exploraré cómo la misma puede afectar al crecimiento económico

"Mucha de la polarización en Europa y las Américas de los últimos 15 años es fruto de la caída del crecimiento económico"

En la sección de economía de la página web de **El Confidencial**, encontramos el artículo **"La inteligencia artificial y el futuro del crecimiento económico"**.

Jesús Fernández-Villaverde, catedrático en Economía de la Universidad de Pennsylvania, y colaborador habitual de la sección, hace en el artículo un resumen sobre el crecimiento de la economía, más concretamente del PIB y sus mecanismos, desde siglos atrás, para analizar posteriormente la posibilidad de la inteligencia artificial pueda doblar el crecimiento de PIB por habitante en economías avanzadas.

Texto completo

PATROCINADORES

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