BOLETÍN Nº53 NOV 2023

AEINSE
Asociación Española de Ingenieros de Seguridad

02 Mensaje de la Junta Directiva

03 NOTICIAS **AEINSE**
AEINSE en la Jornada AESYC
Foro internacional ciberseguridad
Acuerdo ESSIIF-AEINSE
Open show sobre "Smart cities"
25 años Scati

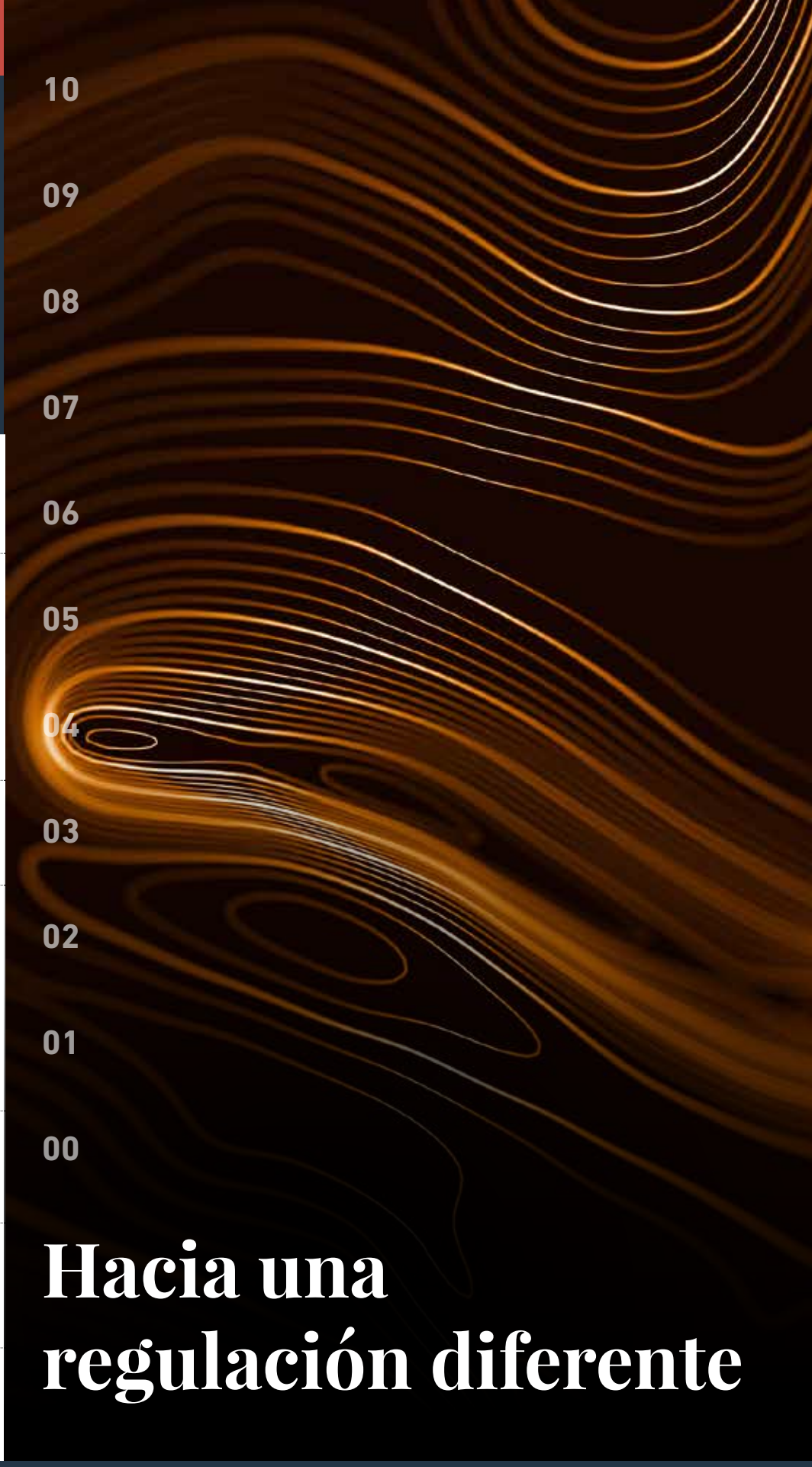
07 NOTICIAS **PATROCINADORES**

16 ARTÍCULO **ESPECIALIZADO**
Cuánto cuesta realmente un Sistema de Seguridad
Ricardo Marranita
Product Growth Manager
AXIS Communications Suecia

22 CONOCE A UN **SOCIO**
Emilio Castro Arroyo

26 **AGENDA** DEL SECTOR

30 **LEÍDO, VISTO Y OÍDO EN...**



Hacia una regulación diferente

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

"En este final de 2023 el sector de la Seguridad llamada Física o tradicional, donde trabajamos (no únicamente) los miembros de AEINSE, sigue en una situación insatisfactoria en lo que respecta a la legislación que le es aplicable."

Hacia una regulación diferente...

Todos conocemos que estamos regulados por una Ley de 2014 que no ha sido desarrollada, por lo que están parcialmente vigentes regulaciones correspondientes a la ley de Seguridad privada anterior, la de 1992, en concreto el Reglamento de 1994 y demás documentos de rango inferior, muy especialmente las órdenes ministeriales de 2011.

Este escenario ha sido de sobra comentado y lamentado, y nos genera algunas inseguridades jurídicas en nuestro quehacer diario y, sobre todo, limitaciones en el desarrollo de soluciones a través de las nuevas tecnologías, amén de disposiciones de medidas de seguridad incoherentes con las amenazas actuales.

Quizá se podrían mencionar, entre otras, situaciones no acordes con la realidad como las de las especificaciones de las medidas de seguridad a aplicar a las CRA con muros y sensores de protección de intrusión y sin ninguna exigencia de protección ante ciberataques, las exigencias de costosas renovaciones de cámaras acorazadas y cajas fuertes en oficinas bancarias que no contienen dinero, la inexistencia de requisitos de control de las empresas de ciberseguridad, etc.

En contraste con esta situación, bien conocida y sufrida por todos, estamos viendo cómo en el sector de la Ciberseguridad se está legislando al dictado de las trasposiciones de las Directivas y Reglamentos Europeos (ver artículo técnico de nuestro boletín nº 51).

Independientemente de otras problemáticas asociadas, esta situación hace que la legislación española que se genera para la Ciberseguridad responda a un enfoque diferente a la que regula la Seguridad Física, con una orientación menos determinista en lo que se refiere a la definición de las medidas de Seguridad a exigir, y más centrada en el Análisis de Riesgos y, en su caso, en certificaciones internacionales.

Nuestra aspiración en ese sentido sería que, a falta de Directivas Europeas sobre Seguridad Física, nuestros legisladores desarrollaran un corpus legal de nuestro sector que no entre en los detalles técnicos tradicionalmente tratados en los documentos legislativos anteriores.

La tecnología es muy rápida en su desarrollo, la necesidad de utilizarla también (drones, Inteligencia Artificial, 5G, Nube...) y, necesariamente, la capacidad de legislar desde la Administración es lenta y, en muchos casos, con insuficientes recursos técnicos.

En **AEINSE** seguiremos intentando desarrollar **Guías de Buenas Prácticas** que ayuden a rellenar los huecos reglamentarios no previstos... pero también necesitamos que lo no previsto no esté prohibido.

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

AEINSE en la Jornada AESYC

AESYC
Alianza Española de Seguridad y Crisis

El pasado 25 de octubre AEINSE participó en la primera Jornada "La labor de las Asociaciones en el sector de la Seguridad Privada. Necesidades, Hoja de Ruta y Objetivos", invitados amablemente por los organizadores del evento, AESYC (Alianza Española de Seguridad y Crisis).

25 OCT 2023

La sesión que se pudo atender de forma telemática, reunió, además de a **AEINSE** a través de nuestro Presidente **Alfonso Bilbao**, a representantes de **ADISPO, ADJSE, ADSI, SEDEXPO, CISEG** y la propia **AESYC**.

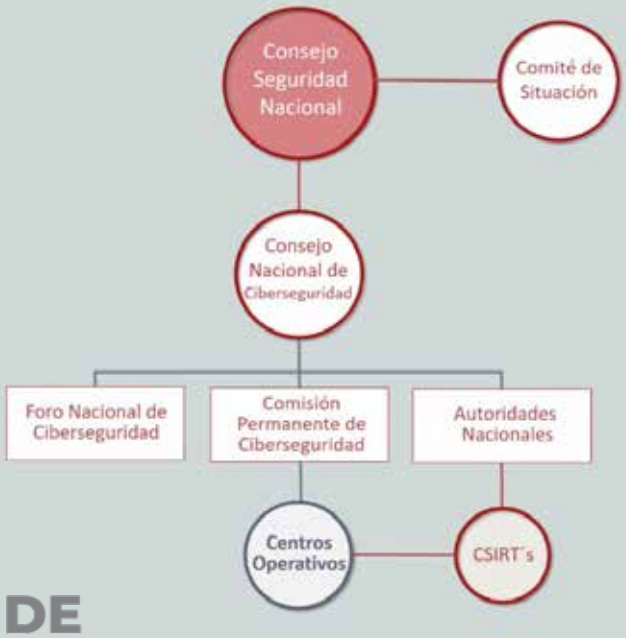
Tras un debate de 90 minutos en el que se evidenciaron los objetivos y actividades de estas Asociaciones, se alcanzaron algunas conclusiones comunes, entre las que cabe destacar:

- El papel de las Asociaciones, siendo relevante, lo debe ser más en la relación con las Administraciones Públicas.
- El diálogo entre Asociaciones, como este acto, es de vital importancia.
- La formación continua es el gran reto de los profesionales de la Seguridad y las Asociaciones han de jugar un papel crucial en ello.

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

Estructura de la Ciberseguridad en el Sistema de Seguridad Nacional



FORO NACIONAL DE CIBERSEGURIDAD

El Foro Nacional de Ciberseguridad es un órgano de asistencia al Consejo Nacional de Ciberseguridad en su condición de órgano de apoyo a su vez del Consejo de Seguridad Nacional.

Su creación se enfoca a que representantes de la sociedad civil, expertos independientes, sector privado, la academia, asociaciones, organismos sin ánimo de lucro, entre otros, colaboren con el objetivo de potenciar y crear sinergias público privadas, particularmente en la generación de conocimiento sobre las oportunidades y amenazas para la seguridad en el ciberespacio.

El **Foro Nacional de Ciberseguridad** está presidido por el **Departamento de Seguridad Nacional** (dependiente de **Presidencia del Gobierno**) y tiene dos Vicepresidencias: el **Centro Criptológico Nacional (CCN)**, órgano del **CNI** y dependiente del **Ministerio de Defensa**) y el **Instituto Nacional de Ciberseguridad (INCIBE)**, dependiente **de Red.es** y por tanto del **Ministerio de Asuntos Económicos y Transformación Digital).** Sus actividades se organizan a través de cinco Grupos de Trabajo:

GT1, Cultura de Ciberseguridad
GT2, Impulso a la Industria y a la I+D+I
GT3, Formación Capacitación y Talento
GT4, Análisis e Impulso a la Industria de Ciberdefensa
GT5, Regulación

En el **GT1**, coordinado por el **Departamento de Seguridad Nacional** y la **Fundación Borredá**, existe el subgrupo **SGT1 "Brújula de la Ciberseguridad del Ciudadano"** en el que se está acometiendo la realización de un documento de gran interés para nuestro sector: la **"Guía para una Seguridad Física Cibersegura".**

Este documento está siendo estudiado y elaborado por un extenso grupo de profesionales, tanto de la industria de la Seguridad y la Ciberseguridad como de la Administración. En su desarrollo está participando activamente **AEINSE**, tanto porque nuestro documento **"G10/21 Guía de Buenas Prácticas de Ciberseguridad en proyectos de Seguridad Física"** forma parte de las aportaciones a estudiar, como por la presencia activa del presidente de **AEINSE**, **Alfonso Bilbao**, en los trabajos que se están realizando.

Sus funciones, organización y servicios que presta se pueden ver **aquí**

Acuerdo ESSIIF-AEINSE

Comienzo de los cursos de seguridad 2023 -2024 tras el acuerdo de ESSIIF- AEINSE

Essiif - Fire @Security School- abre el plazo de matrícula para su **Curso de Especialización en Diseño e Implementación de Sistemas Anti-Intrusión.**

Un **curso de 60 horas** de duración que comenzará el 6 de noviembre. En él se desarrollan las competencias relacionadas con los distintos elementos que engloban la seguridad desde un punto de vista integral y tecnológico, a partir del análisis y estudio de sus diferentes partes: aspectos legales y normativos, gestión del riesgo, gestión operativa de la seguridad, ingeniería y tecnología de los sistemas de seguridad, nuevas tecnologías, ciberseguridad, proyectos en el ámbito de la seguridad, etc.

El área de conocimiento en seguridad de **ESSIIF Security** se ha rodeado para su desarrollo en la **Universidad Isabel I**, como certificadora de los programas formativos y en **AEINSE** como miembro de la organización del itinerario formativo.

+información aquí

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

Open Show
sobre Smart Cities

Organizado por las revistas de la Editorial Borrmart, se celebró el pasado 17 de octubre el Open Show que reúne a profesionales de los sectores de Seguridad, Ciberseguridad, Limpieza, Seguridad Laboral y Facility Management. En esta ocasión centrado en los servicios y tecnologías que afectan a las llamadas Smart Cities.

17 OCT 2023

AEINSE fue invitada a participar en una mesa redonda sobre las tecnologías y necesidades a aplicar de la **Seguridad en las Ciudades Inteligentes.** La Asociación estuvo representada por su Presidente, **Alfonso Bilbao**, que expuso las tecnologías punta aplicables en la actualidad en las ciudades y los retos que implican en materia de formación.

SCATI

El pasado **28 de septiembre SCATI celebró sus 25 años de actividad** con un evento celebrado en Madrid, con el lema "**El viaje comienza aquí**", en el que la empresa mostro su agradecimiento a clientes, colaboradores, asociaciones, publicaciones y otras entidades que han apoyado y exigido a la Compañía para dar lo mejor de sí misma. En palabras de su presidente, **Alfonso Gil**, organizaciones que *"nos han ayudado a crecer e incluso ponernos al límite porque gracias a ello, hemos sido conscientes de lo que somos capaces"*. Como prueba de este agradecimiento, tras la cena, se entregó una placa conmemorativa a diferentes entidades entre las que **AEINSE** se sintió honrada participar y que recogió nuestro vicepresidente de manos de la directora de marketing de **SCATI**.

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

LANACCESS
Discover the power of video.

Tres características únicas de un videograbador para aviónica

En aviones, el circuito cerrado de televisión (CCTV) despliega cámaras en el acceso a la cabina, los pasillos, la bodega y el exterior del aparato. Los videograbadores instalados en las aeronaves graban y almacenan las imágenes y tienen tres aspectos distintivos:

Robustos al extremo

El sector de la aviónica tiene estándares en materia de seguridad, capacidad y eficiencia extremadamente exigentes. Los baremos incluyen: temperatura y altitud; choques operativos, vibraciones; efectos magnéticos; voltajes; susceptibilidad a la radiofrecuencia y emisiones de radiofrecuencia; y efectos directos provocados por el impacto de rayos.

Fuente de alimentación única

Es necesaria una fuente de alimentación adaptada al entorno de una aeronave, que cumpla con las especificaciones referentes a interferencias electromagnéticas, descargas eléctricas, interrupciones de alimentación, bajadas y subidas de tensión, y vibraciones. Además, debe tener una doble función: ha de ser válida tanto para el sistema de grabación como para proporcionar PoE a las cámaras conectadas.

Sistema de configuración automático

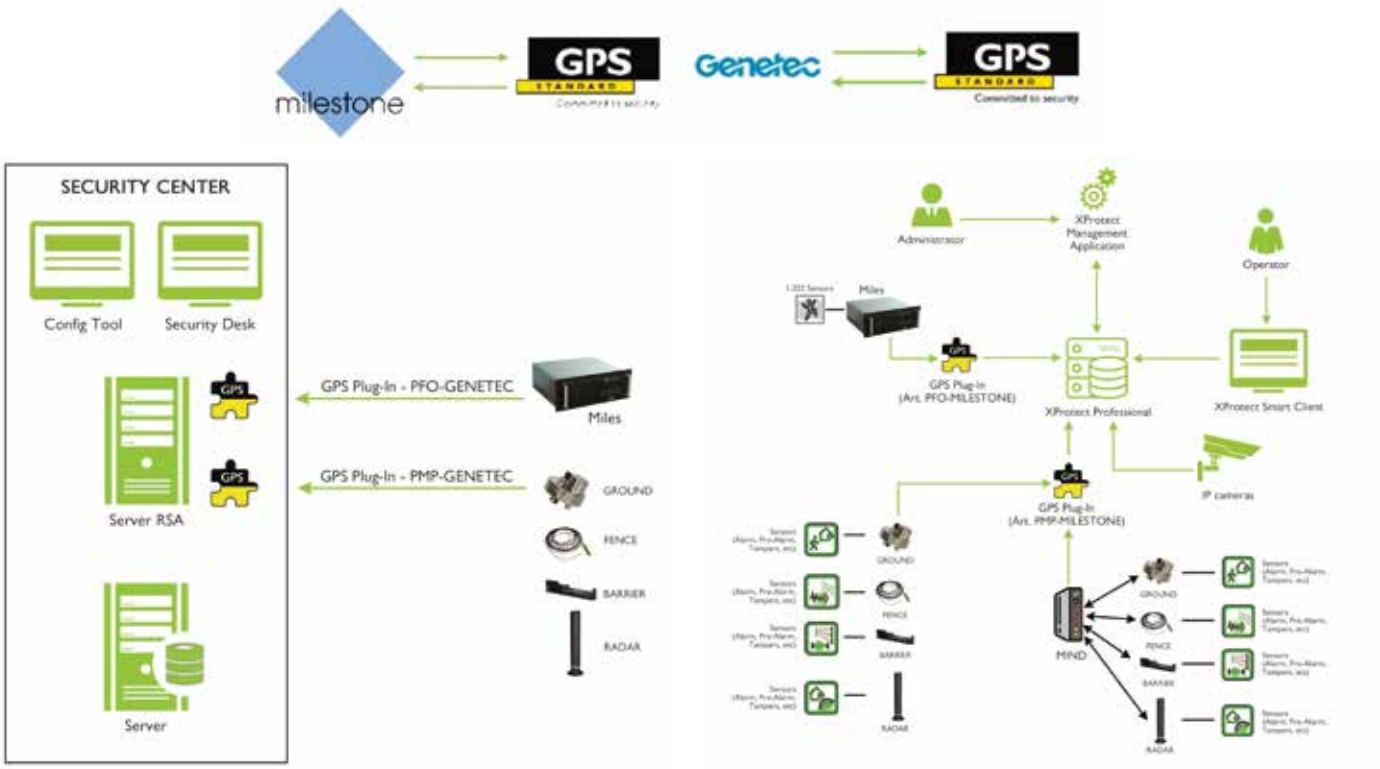
El equipo debe detectar su posición con relación al fuselaje e iniciar un proceso automático de configuración.

En el proyecto de fabricar videograbadores para la aviónica, emprendido en colaboración con un proveedor del sector, **Lanaccess** aplica sus más de 25 años de experiencia diseñando equipos robustos, ciberseguros y eficientes. Además, pone en práctica su consabida capacidad de innovar y adaptar.

Sicuralia

Sensores Perimetrales Integrados con Milestone y Genetec

Sicuralia, ha dado un paso revolucionario al integrar sus avanzados sensores perimetrales enterrados, de vallados y de radar, con las plataformas de VMS de Milestone Xprotect y Genetec RSA. Esta innovadora actualización permite una vigilancia más efectiva y una respuesta más rápida a las amenazas en entornos críticos.



Los sensores perimetrales enterrados y de vallados de **GPS Standard** son conocidos por su capacidad para detectar intrusiones en tiempo real, ofreciendo una seguridad inigualable. La **integración con Milestone** y **Genetec**, brinda a los usuarios un control total sobre sus sistemas de seguridad.

Esta integración permite a los usuarios visualizar eventos en tiempo real, verificando la detección de intrusiones y tomando medidas de manera eficiente. La información se presenta de manera clara y concisa en la interfaz de **Milestone** y **Genetec**, lo que simplifica la toma de decisiones. La colaboración entre **GPS Standard, Sicuralia, Milestone** y **Genetec** marca un hito en la industria de la seguridad, reforzando la capacidad de respuesta y la eficacia de los sistemas de vigilancia perimetral. **Sicuralia** continúa liderando la innovación en el campo de la seguridad, garantizando que sus clientes estén un paso adelante en la protección de sus activos y personas.

+ información **aquí.**

SCATI

Scati Access

Software de Gestión de Control de Accesos

Descubra cómo tener el control total de un entorno seguro

SCATI ACCESS le ofrece la solución completa que necesita para proteger sus instalaciones, integrándose con sistemas de videovigilancia, alarmas o gestión de edificios. De esta forma le garantiza un control completo de la instalación y le permite ofrecer una respuesta rápida en caso de incidentes.

SCATI ACCESS garantiza un nivel de protección sin concesiones. Con cifrado de datos de alto nivel y autenticación de múltiples factores, puede estar seguro de que sólo las personas autorizadas acceden a sus espacios.

Diseñada bajo estándares abiertos, **SCATI ACCESS** está compuesta por un ecosistema de dispositivos hardware y está unida a una plataforma de gestión software.

SCATI ACCESS ofrece diferentes versiones con el objetivo de adaptarse específicamente a las necesidades concretas de cada usuario, manteniendo siempre la máxima escalabilidad para crecer al mismo ritmo que crecen las necesidades de nuestros clientes.

Ya no es necesario comprometer la seguridad, la flexibilidad o la tecnología cuando se trata de control de accesos. **SCATI ACCESS** le ofrece la solución completa que necesita para proteger su edificio y gestionar el acceso de manera eficiente.

+ INFORMACIÓN aquí.

AXIS COMMUNICATIONS

Axis Communications ha anunciado el lanzamiento del AXIS W400 Body Worn Activation Kit, una nueva incorporación a su gama de productos wearable. El AXIS W400 Body Worn Activation Kit pone en marcha automáticamente la grabación en todas las cámaras corporales del mismo sistema cuando se activa una barra de luces o una sirena o al pulsar un botón de pánico.

Nueva cámara corporal W400

En situaciones de estrés, es fácil que los usuarios de cámaras corporales olviden poner en marcha la grabación. Con el **AXIS W400** este riesgo desaparece: el kit activa la grabación en una o varias cámaras cuando hay algún incidente, lo que permite a la policía cumplir con sus obligaciones legales y evitar demandas de responsabilidad.

Al integrar el **AXIS W400** en un coche de policía, el sistema puede activarse automáticamente cuando se pone en marcha la barra de luces o la sirena. Y también puede conectarse a un botón de pánico, por ejemplo, en tiendas para activar las grabaciones automáticamente.

Principales características:

- **Activación automática de las grabaciones**
- **Accionamiento desde el propio kit de todas las cámaras conectadas al mismo**
- **Todos los elementos del kit están conectados por Bluetooth**

El **AXIS W400** empezará a comercializarse a través de los canales de distribución de Axis en el cuarto trimestre de 2023.

+información **aquí.**

Seguras por defecto

Cámaras Bosch

BOSCH

El aumento de sistemas IP conectados, las recientes certificaciones en ciberseguridad, unido a la creciente demanda de mecanismos de protección, obligan a establecer unas medidas de seguridad por defecto, en lugar de tener que hacerlo durante la configuración.

A partir de las versiones de firmware 9.0, 8.90 y 7.88, en sus respectivas plataformas, Bosch adoptará una de las mejores prácticas de ciberseguridad al desactivar ciertos puertos de la cámara de forma predeterminada.

Los siguientes puertos, **RCP+ (1756), HTTP (80), RTSP (554)** y Servidor iSCSI (3260), estarán deshabilitados y deberán tomarse las medidas oportunas usando el túnel HTTPS y configurando los clientes de forma adecuada.

A esta medida se le unen las ya exitosas:

- **Chip Secure Element soportando llaves de seguridad de hasta 4096 bits.**
- **Firewall de inicio integrado, evitando ataques DDOS.**
- **Contraseña obligatoria en el inicio.**
- **Mínima versión de TLS 1.2.**
- **SCEP: para una integración más sencilla de infraestructuras de clave pública y certificación digital.**
- **Sellado del software con el fin de proteger de cambios no autorizados en la configuración.**
- **El certificado Bosch para la firma y encriptado del firmware evita cargas de firmware malicioso.**
- **Chequeo de actualizaciones en el Cloud.**
- **Establecimiento del tiempo de conexión de configuración desatendida.**
- **Y las certificaciones UL-2900-2-1, IEC62443-4-1 e IoT SMM.**

Matrix One

La escalabilidad, clave para lograr un sistema de control de acceso a tu medida

dormakaba

MATRIX ONE, la solución de acceso basada en la web -y próximamente también en la nube- que dormakaba ofrece a los instaladores de seguridad, se presenta como la respuesta a todas las necesidades de acceso que puedan tener las pequeñas y medianas empresas.

Gracias a su software modular y escalable, ofrece tres diferentes opciones de acceso en función del tamaño de la compañía.

MATRIX ONE S: la opción ideal para gestionar hasta 100 usuarios y puertas. Disponible en online y offline, incluye la opción de mobile Access y un plan de cierre sencillo.

MATRIX ONE E: gestiona hasta 4 millones de usuarios y puertas ilimitadas. Permite crear perfiles de acceso, incluir código PIN, huella y reconocimiento de matrículas y tiene disponible el acceso al módulo de ascensores. Además, admite realizar correcciones masivas.

MATRIX ONE O: la opción más completa. Facilita información sobre el estado de las puertas y el aforo de las salas. Además, posee una interfaz para interactuación con sistema de intrusión, un sencillo módulo de control de presencia y permite la gestión de alertas y exportar e importar datos. Su función "inquilinos" admite hasta 5 instalaciones por empresa.

El sistema cumple con las últimas normas de control de acceso y es compatible con todo el porfolio de dispositivos **dormakaba** -controladoras, lectores, cilindros y manetas digitales- además de integrarse, también, con algunos terminales de terceros.

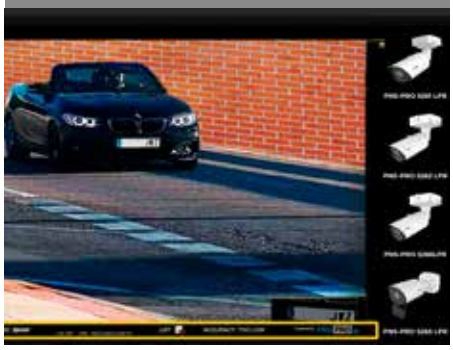
Con **MATRIX ONE** el acceso siempre es fácil.

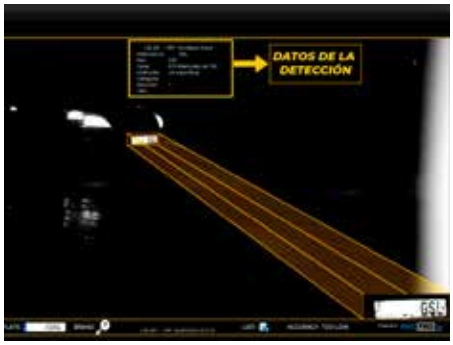
+ información aquí.

Cámaras LPR PNS-PRO
de reconocimiento de matrículas

Evolucionando la gestión del tráfico con la gama de cámaras LPR PNS-PRO:

VIDEOSISTEMAS FFV GEUTEBRÜCK





En respuesta a la creciente congestión del tráfico, accidentes, desafíos de estacionamiento y supervisión de aparcamiento, presentamos las cámaras LPR PNS-PRO, una solución avanzada para una gestión efectiva del tráfico. Estas cámaras son capaces de reconocer matrículas en vehículos a velocidades de hasta 200 km/h, capturando fotogramas a alta velocidad durante el día y la noche con un 95% de certeza.

Impulsadas por algoritmos de inteligencia artificial, van más allá al captar atributos adicionales, detectando además tipo, color y marca del vehículo en cada reconocimiento. Con esta funcionalidad en la plataforma **Geutebrück** podrá optimizar la gestión permitiéndole realizar búsquedas detalladas y trazabilidad de los vehículos, mejorando la eficiencia operativa en todas las instalaciones.

Las cámaras gestionan listas blancas y negras para ejecutar acciones: apertura automática de barreras, notificación de intentos de acceso de vehículos no autorizados, interacción con sistemas de control y gestión de tráfico.

Destacamos su capacidad para detectar vehículos sin matrícula y aquellos que circulan en sentido contrario, proporcionando datos cruciales para la seguridad vial. Las cámaras **LPR PNS-PRO** son una respuesta eficaz a los desafíos actuales en la gestión del tráfico, ofreciendo una mejora sustancial en la seguridad y eficiencia tanto para las carreteras, como para la gestión de vehículos en instalaciones privadas.

+ información aquí

Nuevos Domos PTZ Plus
con Inteligencia Artificial

Hanwha Vision, ha lanzado una gama de cámaras PTZ con Inteligencia Artificial para ofrecer una detección y clasificación precisas. La inclusión de la Inteligencia Artificial reduce las falsas alarmas y permite que las cámaras clasifiquen con precisión objetos: personas, rostros, vehículos (diferenciando el tipo de vehículo) y matrículas.

Esta detección y clasificación permite a los operadores una búsqueda forense muy eficiente. En combinación con el análisis de vídeo, los operadores pueden supervisar objetos que entran y salen de una zona predefinida o que cruzan una línea.

La Inteligencia Artificial con Deep Learning implica que las cámaras ignoran objetos irrelevantes, como hojas de árboles, nubes o animales (falsas alarmas). Esto permite a los operadores centrarse en incidentes reales.

Las cámaras **AI PTZ PLUS** pueden trabajar con otros dispositivos y sensores mediante **MQTT**. Por ejemplo, un desplazamiento automático a una entrada/salida para proporcionar una confirmación visual u, opcionalmente, la cámara puede compartir información sobre una detección de objetos para activar acciones específicas (bloqueo de puertas o encender luces). La capacidad de comunicarse y compartir datos a través de **MQTT** transforma las cámaras **AI PTZ PLUS** en una Solución de Inteligencia Empresarial.

Las nuevas cámaras de 2 MP, 6 MP y 4K pueden capturar imágenes de tipo pericial de objetos hasta una distancia de 200 metros en todas las condiciones de iluminación, gracias a la tecnología IR adaptativa.

+ información aquí

NUEVA Cámara de Doble Sensor Illustra IQ

Johnson Controls Security Products, se enorgullece en presentar el lanzamiento de su innovadora Cámara de Doble Sensor Illustra que redefine la tecnología de videovigilancia.

Johnson Controls

Esta cámara de vigilancia de última generación está diseñada para romper barreras y elevar los estándares de la industria. Gracias a su combinación única de 2 sensores con óptica varifocal de 5 o de 8 megapixels cada uno, ofrece un rendimiento excepcional y una amplia gama de características avanzadas.

- **Un procesador de Inteligencia Artificial (AI) individual para cada uno de los sensores.**
- **LEDs IR con alcance de 35m. individual en cada sensor.**
- **Fácil instalación.**
- **Máximos niveles de características de ciberseguridad además de encriptación punto a punto.**
- **Apta para uso exterior IP66.**
- **Formato de orientación de imagen "modo pasillo".**
- **Máxima rentabilidad al requerir un único punto de conexión PoE y una única licencia en el sistema de gestión de vídeo VMS.**

Una de las grandes innovaciones es el nuevo formato de cámara con 2 sensores independientes que permite un mayor campo de visión en situaciones tales como a lo largo de pasillos, zonas en esquina, descansillos de escaleras, recepción de edificios, etc.

En todos los casos optimizando el campo de visión desde un único punto de instalación, que puede ser en techo o en pared y facilitado además con las múltiples características de ajuste individual de cada uno de los sensores. Con este nuevo formato de cámara se redefinirá el futuro del diseño de los proyectos de videovigilancia.

+ información aquí

¿CUÁNTO CUESTA REALMENTE UN SISTEMA DE SEGURIDAD?

Ricardo Marranita

PRODUCT GROWTH MANAGER EN AXIS COMMUNICATIONS SUECIA

ricardo.marranita@axis.com

A la hora de comprar un sistema de seguridad, las decisiones suelen condicionarse al precio de los equipos, su instalación y puesta en marcha. Pero adoptar este enfoque puede dejar al usuario final con grandes retos por delante. Los sistemas de vigilancia pueden durar entre cinco y veinte o más años, por lo que condensar todas las consideraciones de costos en el gasto inicial no tiene en cuenta el panorama general.

De hecho, los costos iniciales de comprar, instalar y configurar un sistema de seguridad tienden a representar solo el 30% de los costos totales experimentados durante la vida útil del sistema, costos conocidos como Costo Total de Propiedad.

A pesar de esto, muchos usuarios finales pueden tomar su decisión basándose únicamente en estos costos iniciales, muchas veces con solo una visión del 10-15% de los costos totales del sistema de seguridad. La realidad es que aproximadamente el 70% de los gastos se producen después de que se haya instalado el sistema. Lamentablemente, esto puede ser una sorpresa desagradable para aquellos usuarios finales que no han considerado los costos indirectos del sistema de seguridad.

Tomarse un tiempo para pensar en cómo se utilizará el sistema y los costos asociados con ese uso puede generar ahorros significativos a largo plazo.

CUÁNTO CUESTA UN SISTEMA DE SEGURIDAD

Las elecciones iniciales, como el tipo de dispositivo que se va a implementar, afectan a los gastos futuros, desde el consumo de energía hasta la operación y el mantenimiento. Aunque **aquí nos centraremos específicamente en un sistema de videovigilancia**, este principio se aplica a cualquier sistema de seguridad. Tener en cuenta el coste total de propiedad ayudará a identificar las preguntas que debe hacerse a la hora de tomar una decisión sobre qué nuevo sistema de seguridad comprar.

Tomando como ejemplo el sistema citado, mirar más allá del precio de las cámaras es un paso importante en el proceso de compra: establecer sus requisitos de vigilancia y el presupuesto disponible es clave para reducir las opciones de compra.

Desafortunadamente, demasiadas conversaciones iniciales sobre los requisitos se centran únicamente en las cámaras, sin tener en cuenta los requisitos más amplios del sistema en su conjunto; desde el uso de energía hasta las necesidades de almacenamiento. Puede ser tentador centrar en las cámaras la conversación sobre el presupuesto, en lugar de dónde se tendrá que gastar el dinero para operar y mantener esas cámaras.

Sin embargo, el sistema de seguridad tendrá que satisfacer sus necesidades en el futuro previsible. Vale la pena recordar que los costos de operación, monitoreo y mantenimiento de ciertas cámaras a menudo exceden los propios dispositivos y, por lo tanto, deben sopesarse antes de realizar la compra.

Previsión de los costos de almacenamiento

En general, todo sistema de videovigilancia requiere considerar cómo almacenar las imágenes una vez grabadas. En promedio, la legislación exige que las pruebas potenciales se almacenen durante un mes. Sin embargo, en algunas regiones o casos de uso, este plazo puede extenderse, lo que hace que el almacenamiento sea un factor considerable en los costos generales del sistema de seguridad.

Para evitar verse atrapado con gastos significativos de servidores después de instalar las cámaras, es fundamental considerar los diferentes costos de almacenamiento asociados con cada modelo de cámara que se está evaluando. Puede ser una falsa economía comprar cámaras más baratas para reducir el desembolso inicial si vienen con grandes requisitos de almacenamiento, lo que obliga a gastar más en servidores y a largo plazo mayores costos recurrentes.

Por otra parte, si se pretenden reducir los costos de almacenamiento reduciendo el tamaño del video almacenado, se deberán elegir cuidadosamente los dispositivos para asegurarse que la compresión del video no comprometa la calidad al pixelar o difuminar las imágenes hasta el punto de que ya no sea posible identificar a un sospechoso. En esencia, terminar con imágenes de mala calidad que no sirvan como evidencia útil.

Algunas cámaras poseen tecnología sofisticada que puede preservar todos los detalles forenses importantes que se necesitan, como rostros, tatuajes o números de matrícula, y eliminar solo los datos innecesarios. Eso permite que las cámaras funcionen al máximo, al mismo tiempo que reducen los requisitos de ancho de banda y almacenamiento en 50%-95% en comparación con la compresión estándar, y, por lo tanto, reducir los costos a largo plazo. Vale la pena verificar cualquier afirmación de imágenes de alta calidad con bajos requisitos de almacenamiento antes de instalar el sistema para asegurarse de que cumpla con las expectativas.

Estimar el costo de uso y funcionamiento del sistema

También es importante preguntarse: ¿qué sucede una vez que el sistema está en funcionamiento? Este paso a menudo se pasa por alto: algunos pueden aceptar los costos operativos del sistema como el costo natural de hacer negocios, mientras que otros pueden no pensar demasiado en ello si termina bajo el presupuesto de otro departamento.

Sin embargo, dedicar algo de tiempo a pensar en los costes necesarios para mantener el sistema en funcionamiento es donde se producen las mayores pérdidas. Si bien es posible que no le afecte al departamento de seguridad directamente, afecta a la compañía.

Por lo tanto, considerar el uso de electricidad, el mantenimiento requerido y los costos para monitorear el sistema es importante.

Es necesario preguntarse:

- ¿Cuánta energía consumen estas cámaras durante su uso y cómo afecta eso a su factura de electricidad?
- ¿Cuánto almacenamiento necesita para estas cámaras específicas y cómo afecta eso a sus costos de electricidad, sin olvidar el consumo de la climatización, a largo plazo?
- Los costos de mantenimiento de hardware y software.
- La funcionalidad inteligente para reducir los costes de monitoreo y búsquedas forenses, así como la minimización de las falsas alarmas a fin de reducir los costos operativos.

Los dispositivos que se elijan afectarán en última instancia a todos los costos que se producirán a lo largo del ciclo de vida del sistema de seguridad.

Predecir el impacto que el sistema tendrá en el negocio

El análisis no debe reducirse únicamente a los costos. Una vez que se hayan trazado las implicaciones de costos generales para todo el sistema, cabe preguntarse: ¿cómo ayudará el sistema al negocio? ¿Impulsará una mayor eficiencia, reducirá los robos, mejorará el servicio que brinda a los clientes, mejorará la retención de empleados al crear un lugar de trabajo más seguro?

En última instancia, el sistema de seguridad correcto para una organización puede crear valor empresarial, lo que se traduce en mejorar los resultados. Es importante cuantificar cómo afectará el sistema de seguridad al negocio para que se puedan sopesar esos beneficios con los costos totales al tomar su decisión.

COSTO TOTAL DE PROPIEDAD

El **Costo Total de Propiedad TCO** (por sus siglas en ingles, **Total Cost of Ownership**) contempla los costos de compra e instalación inicial y los costos a lo largo de la vida útil del bien adquirido incluyendo, entre otros, los siguientes conceptos:

- **Valor de compra inicial**
- **Instalación y configuración**
- **Formación a los usuarios**
- **Gastos legales y licencias (si aplican)**
- **Mantenimiento del sistema**
- **Actualización de software**
- **Consumo energético**
- **Costos de desecho al final de su vida útil**

Elegir el socio adecuado para la compra y desarrollo del proyecto

Es fundamental encontrar el socio adecuado que ayude a la compañía a analizar los escenarios citados para encontrar el sistema que mejor se adapten, tanto en términos de coste total de propiedad, como en la funcionalidad del sistema para que cumpla con los requisitos capaces de generar valor a largo plazo.

Algunas acciones que ayudarán a reducir los costos de propiedad en el momento del diseño del sistema

Optimización de iluminación adicional

La mayoría de los sistemas de vigilancia deben ser capaces de proporcionar imágenes de alta calidad en la oscuridad. Una opción es comprar, instalar y alimentar iluminación adicional para respaldar el sistema de seguridad, pero esto aumentará las facturas de energía y el mantenimiento. Alternativamente, algunos programas de cámara compensan los bajos niveles de luz aumentando la ganancia, pero esto aumenta los requisitos de almacenamiento y los costos de electricidad de equipos. Dada la medida en que las facturas de electricidad están aumentando debido a la crisis energética actual, es vital encontrar formas de reducir los requisitos de iluminación y electricidad sin comprometer el rendimiento del sistema.

Vale la pena considerar las tecnologías de optimización de la luz que no tienen el mismo impacto a gran escala en los costos de almacenamiento o no requieren la instalación de iluminación adicional. Tecnologías que combinan sensores extremadamente sensibles y un procesamiento de imágenes cuidadosamente ajustado, ofreciendo vídeo de alta resolución a todo color con un mínimo de desenfoque de movimiento, incluso en la oscuridad. Capturando grandes detalles con muy poca luz, creando una excelente calidad de imagen sin necesidad de fuentes de luz externas.

Otra posible solución para minimizar la necesidad de iluminación adicional es utilizar iluminación infrarroja integrada en la cámara que se adapta automáticamente, ampliándose o estrechándose a medida que la cámara se acerca y se aleja, por lo que todo el campo de visión se ilumina de manera uniforme y se optimiza el consumo.

También puede disminuirse el consumo utilizando una cámara con un radar asociado, de manera que la iluminación se activa únicamente cuando el radar detecta movimiento y no durante toda la noche. Además se conseguirá mejora en la verificación y mantener las falsas alarmas al mínimo.

Reducción de las facturas de mantenimiento

Para garantizar que las cámaras puedan hacer lo que necesita que hagan a lo largo del tiempo, se necesitan actualizaciones periódicas de software y mantenimiento del hardware en buen estado, así como la limpieza de carcasas y ópticas. Esto suena simple, pero estos pasos a menudo se pueden pasar por alto, tanto en términos de mantenerse al tanto de ellos como de ver dónde se pueden ahorrar.

Suena obvio, pero las cámaras de vigilancia necesitan una visión clara de una escena si quieren hacer su trabajo correctamente. La suciedad, el polvo, las telas de araña y otros eventos pueden acumularse para bloquear la vista, además de provocar problemas de sobrecalentamiento y posibles fallos en los componentes si no se abordan adecuadamente.

Desafortunadamente, el costo de limpiar manualmente las cámaras puede aumentar, especialmente si los dispositivos se encuentran instalados en altura y en entornos con mucha suciedad y polvo. Por ejemplo, los sistemas de vigilancia instalados en condiciones ambientales difíciles, como una plataforma petrolífera en alta mar o una planta química, pueden generar importantes facturas de mantenimiento para limpiar continuamente el agua salada y el polvo de las cámaras. Por otra parte, también se pueden necesitar de elementos de elevación y consideraciones de riesgos laborales exigentes.

Para combatir estos costes, se puede optar por la posibilidad de invertir en cámaras que ofrecen funciones de limpieza remota, o diseñadas con materiales y componentes autolimpiantes o con capacidad de eliminar el agua del objetivo.

Por otra parte está el mantenimiento que podríamos llamar digital. Cada día se encuentran nuevas vulnerabilidades. Cuanto más tiempo permanezca desactualizado el software o firmware, mayor será el riesgo para la organización.

Sin embargo, es difícil mantenerse al tanto de las actualizaciones de software de manera eficiente cuando se trata de cientos o incluso miles de dispositivos. Se hace necesario disponer de los mecanismos de información correctos con fabricantes y mantenedores y disponer de herramientas remotas de gestión de los dispositivos que no obliguen a recurrir al campo, reduciendo drásticamente los tiempos y, por tanto, los costos de las actualizaciones.

Todos estos detalles pueden parecer abrumadores. Lo más importante es empezar poco a poco, con los temas más cómodos. Siempre y cuando se obtenga una nueva perspectiva de este proceso, se está dando un paso en la dirección correcta: pasar de comprar un sistema de seguridad a hacer una inversión que puede cosechar mejores recompensas para toda la organización. ¡Buena suerte!

CONOCE A UN

SOCIO

Emilio Castro Arroyo

SOCIO Nº 151

peritoemilio@gmail.com

Buenos días Emilio, lo primero es pedirte que te presentes al resto de socios para que podamos conocerte.

Buenos días Carlos. Me llamo Emilio Antonio Castro Arroyo y, si bien soy jiennense de nacimiento, llevo ya en torno a 20 años viviendo en Madrid. Vine a estudiar aquí y, tras finalizar mis estudios universitarios, me quedé trabajando.

¿Cuál es tu formación académica?

Soy Ingeniero Técnico Industrial en la rama de Electrónica Industrial e Ingeniero Técnico de Telecomunicaciones en la rama de Sistemas Electrónicos. Estoy habilitado por el Ministerio del Interior como Director de Seguridad y Jefe de Seguridad, con TIP en vigor, y tengo formación como Perito Judicial.

Me consta que siempre te has preocupado y ocupado de la formación ¿Qué otros cursos has seguido una vez finalizada la ingeniería?.

En cuanto al sector que nos ocupa y en el que desarrollo mi actividad actualmente, que son los Sistemas Electrónicos de Seguridad, he realizado y sigo realizando periódicamente multitud de cursos en diferentes tecnologías y de diferentes fabricantes de sistemas de Intrusión, Circuito Cerrado de Televisión y Control de Accesos.

De sobra es conocida por todos nosotros la elevada velocidad de progreso de las nuevas tecnologías y, por lo tanto, también de obsolescencia de sistemas ya existentes. Aparte, los delincuentes cada vez adquieren un nivel más alto de especialización y, por desgracia, también disminuye el número de agentes de las FFCCS en las calles. Además de cursos relacionados con el sector de la Seguridad y con otros campos, tengo también bastante formación en el ámbito de la Prevención de

Riesgos Laborales, dados la obligatoriedad legal y los entornos en los que desarrollo mi trabajo en muchas ocasiones: Infraestructuras Críticas, entornos industriales, instalaciones de generación, transporte y distribución de electricidad, etc.

La última que he finalizado este año ha sido un Programa de Liderazgo Estratégico para Directivos en ESADE de 6 meses de duración, organizado por la empresa en la que trabajo actualmente: Ilunion Seguridad.

Recientemente he comenzado una formación para certificarme dentro de unos meses como Project Management Professional por el Project Management Institute.

De las formaciones cursadas ¿Cuál te resultó más interesante y cuál te ha resultado más útil?

La más interesante y que a la vez me resultó más útil fue la primera que cursé sobre sistemas de Intrusión impartida por un fabricante, y supuso mi primera experiencia con el mundo de la seguridad, mi primera toma de contacto con esta disciplina.

Durante mi etapa universitaria nunca recibí formación en Sistemas Electrónicos de Seguridad, pero posteriormente, iniciada ya mi vida laboral, me ví obligado a formarme en ella ya que una empresa en la que trabajé, además de instalaciones eléctricas de BT y MT y redes de voz y datos en entornos CPD, empezó a comercializar la instalación de Sistemas Electrónicos de Seguridad.

Por aquel entonces, mi puesto era el de un ingeniero junior/jefe de obra, y en la Compañía surgió la necesidad de aprender a diseñar Sistemas de Seguridad, así como de presupuestarlos y ponerlos en marcha.

¿En qué empresas has desarrollado tu actividad profesional y cuáles son, o eran, sus sectores, así como qué cargos desempeñaste?

Empecé en una empresa instaladora del sector eléctrico, Dominios Eléctricos, redactando proyectos de instalaciones de Media y Baja Tensión para empresas de construcción: líneas aéreas y subterráneas de electricidad, transformadores, sector fotovoltaico, electrificación de polígonos industriales, naves industriales, urbanizaciones, viviendas.

Posteriormente me encargaba de realizar los boletines de instalación y la legalización de los proyectos en la Administración (Delegaciones de Industria) y en las Compañías suministradoras, y ya seguí con la Dirección Facultativa de este tipo de instalaciones: certificaciones, control de personal propio y subcontratas y control de calidad de las instalaciones.

Posteriormente salté al sector de las redes de voz y datos en entornos data center, en la empresa ARX Soluciones Integrales. Aquí fue donde tuve mi primer contacto con el mundo de la seguridad, como he explicado antes. Ya era necesaria la instalación de sistemas de control de accesos a los centros de proceso de datos y la monitorización del trabajo de los operarios en su interior con sistemas de CCTV, así como la securización frente al robo de las zonas de almacenamiento en las que se guardaban servidores informáticos, gran cantidad de cable de cobre, herramienta valiosa, etc.

En este sector estuve trabajando hasta el inicio de la crisis financiera internacional de las hipotecas subprime de 2.007-2.008, que provocó el cierre de la Compañía en la que trabajaba, y empecé en un gabinete pericial especializado en la detección del fraude a las Compañías de Seguros.

Superado ya el periodo de recesión económica mundial, seguí exclusivamente en el sector de la seguridad, en empresas como Johnson Controls GWS, Envitel Tecnología e Inerco Securiy, tanto diseñando Sistemas Electrónicos y redactando proyectos, como realizando la instalación, configuración y puesta en marcha de las instalaciones, principalmente en entornos de Infraestructuras Críticas e industriales.

Actualmente ocupo el puesto de Ingeniero Jefe de Operaciones de Sistemas de Seguridad en Ilunion Seguridad.

Cuando trabajaste en Envitel Tecnología te ocupabas de proyectos en África y Europa. ¿Qué diferencias más notables encontraste entre la gestión de obra y clientes entre Europa y África?

En Europa: los clientes (sus riesgos, sus necesidades, costumbres, y el concepto de la Seguridad en sí mismo) suelen ser similares a los que tenemos en nuestra Patria. Ídem con la gestión de obra: no supone problema alguno el envío de cualquier tipo de material desde España a cualquier país de la UE ni de facturación de los trabajos realizados o la adquisición de cualquier herramienta que pueda ser necesaria durante su ejecución. Es relativamente fácil comprometerse con una fecha de entrega de obra porque tienes casi garantizado el suministro del material necesario con la calidad esperada, así como la mano de obra necesaria para ello.

En África, los clientes suelen ser muy exigentes con las fechas de inicio y finalización de obra, pero a la vez, todo es muy etéreo también. Los protocolos sociales y empresariales son diferentes y algo que para nosotros puede considerarse intranscendental, en esas zonas puede constituir una grave ofensa o incluso un delito penal, y a la inversa para nosotros.

En cuanto a gestión de obra, no siempre hay electricidad, ni combustible de calidad ni agua potable disponible. El simple consumo de agua de un cubito de hielo sin las debidas garantías puede suponer el contagio del cólera, a ti y a todo tu equipo, o el contagio de malaria de por vida por un mosquito. Los periodos de ayuno y oración durante el Ramadán deben ser tenidos en cuenta en el desarrollo de las obras si hay trabajadores musulmanes.

Hay que tener todos los aspectos muy bien definidos: contratación o no de mano de obra en destino, trámites aduaneros de materiales y herramienta, adquisición de materiales en destino en caso de haberlos, transporte desde España hasta país de destino (coste económico, containers, puertos de salida y llegada, packing list, inspecciones aduaneras en destino), alojamiento, seguridad personal y seguros de salud/accidentes/repatriación en caso necesario.

Recuerdo especialmente la epidemia de ébola de 2015, fecha en la que me encontraba realizando una instalación enorme de control de accesos y CCTV en Togo.

La mayoría de los recuerdos y experiencias que tengo de mis viajes y estancias allí son buenos, y aún conservo y mantengo contactos en algunos países: no me importaría volver algún día. Sé que hay necesidad de Sistemas de Seguridad allí y que los clientes que los solicitan disponen de solvencia económica suficiente.

Antes de llegar a la seguridad has trabajado en el sector eléctrico y haciendo peritajes e informes técnicos. ¿Cómo de útiles te han resultado los conocimientos adquiridos en el primero para llevar a cabo los peritajes?

Han sido muy útiles: para redactar un Informe Pericial que va a estudiar un juzgador que carece de conocimientos técnicos, y que va a ser tenido en cuenta para dictar una sentencia (absolutoria, condenatoria, o del tipo que sea), es imprescindible ser un experto en la materia sobre la que se está discutiendo.

En mi caso, los conocimientos de electricidad y de Sistemas Electrónicos de Seguridad, así como en los Reglamentos y legislación asociados a dichas disciplinas, son fundamentales para poder explicar a los Tribunales de una forma independiente y, sobre todo, comprensible, el porqué de la ocurrencia de un suceso, y las acciones y omisiones de todos los actores intervinientes en un evento sea del tipo que sea: un robo, un incendio, etc.

No solo he hecho Informes Periciales sobre electricidad o Sistemas de Seguridad a lo largo de mi vida: la mecánica es otra rama que siempre me ha gustado mucho y con la que he disfrutado redactando Informes para clientes finales o Gabinetes de Abogados.

¿Cuáles consideras que son tus puntos fuertes?

Me caracterizan la ética profesional, mi responsabilidad, capacidad de trabajo y el compromiso con los clientes y empresas para las que desarrollo mi trabajo.

En tu trabajo actual de Ingeniero Jefe de Operaciones de Sistemas de Seguridad ¿Cuál es tu relación con la gestión de la ciberseguridad de las instalaciones?

La ciberseguridad es una de las principales incorporaciones en la transformación digital de los últimos tiempos. El incremento exponencial de las aplicaciones de Sistemas de Seguridad en cloud implica nuestra colaboración diaria con los Departamentos de IT/TIC de los clientes públicos y privados.

La ciberseguridad se contempla desde el desarrollo mismo del proyecto: al hacer el diseño de los Sistemas y la selección de los componentes/fabricantes que los formarán, continúa posteriormente con los citados Departamentos de los clientes, y con el nuestro propio como proveedores de servicios y Sistemas de Seguridad globales, cuando un proyecto ya está ejecutado y proporcionando la solución para la que ha sido diseñado.

A la hora de contratar técnicos o buscar subcontratas ¿Qué formación y habilidades buscas en ellos?

En cuanto a los técnicos se refiere, busco en ellos responsabilidad y ACTITUD por encima de la APTITUD: no me preocupa que un técnico de Sistemas Electrónicos de Seguridad no sea un experto en su campo o carezca de ciertas certificaciones, pero sí me preocupa que no tenga una actitud positiva ni ilusión por el aprendizaje, o que carezca de inquietu-

des por él. Un buen técnico de Sistemas Electrónicos de Seguridad ha de tener conocimientos de electricidad, electrónica, informática, telecomunicaciones y normativa legal, si bien tengo claro que todo no puede ser imprescindible ni es fácil que alguien lo reúna.

La responsabilidad, como ya he dicho, así como la flexibilidad y la absoluta discreción con los datos que manejan, sí son fundamentales: deben tener claro que se dedican a un sector que en ciertas ocasiones exige dedicación, por la necesidad de atender servicios de guardia para instalaciones o clientes críticos, en fechas y horarios a veces intempestivas, en los que una avería o una incidencia en los Sistemas puede dejar la seguridad de una instalación o de las personas a la deriva, a merced de los delincuentes, o de un eventual incendio, incluso provocando la necesidad de montar un servicio de vigilancia física, con el coste que ello implica.

Lo ideal sería que, en vez de un trabajo para él, su labor como técnico la entendiera como una ocupación, algo con lo que disfrutara y que comprendiera que con su profesionalidad resuelve un problema o una necesidad de seguridad vital para los clientes.

En cuanto a las subcontratas, es imprescindible que estén legalmente homologadas para la instalación y el mantenimiento de Sistemas de Seguridad, tal y como obliga la legislación vigente. Además, valoro muy positivamente que su personal técnico disponga de toda la formación posible en materia de Prevención de Riesgos Laborales, así como certificaciones para mantenimiento de Sistemas de Protección Contra Incendios y en la instalación y puesta en marcha de sistemas electrónicos de seguridad de los fabricantes más habituales.

Las subcontratas deben ser responsables con el trabajo encomendado en cuanto a plazos de finalización y calidad de la instalación realizada (etiquetado, documentación as built, ordenamiento y terminaciones de cableado, así como correcta ejecución de las canalizaciones). Igualmente, me gusta la discreción y fluidez en la comunicación con sus responsables para poner de manifiesto cuanto antes los problemas que inevitablemente surgen en todas las obras, y poder consensuar cuanto antes una solución. Todos los contratiempos deben ser transparentes para el cliente final.

Como todo no debe ser trabajar, seguro que sacas algo de tiempo para desarrollar otras aficiones. Háblanos de ellas.

Debido a mi puesto de trabajo, tengo un nivel de estrés elevadísimo. Viajar en moto con mi mujer y, cuando puedo, acompañado de mis padres, que también conducen la suya propia, hacen que mi presión arterial descienda a valores normales y pueda conciliar el sueño sin dificultad.

En invierno practico el deporte de la caza, entendida como una excusa para salir a pasear por el campo, reunirme y charlar distendidamente con mis amigos, mientras degustamos posteriormente las piezas que hayamos podido cazar.

¿Qué viste en AEINSE para decidir hacerte socio?

Una Asociación debidamente registrada como tal, formada por un grupo de compañeros repartidos por todo el país, ingenieros con experiencia en seguridad debidamente acreditada, con un código deontológico, que podían aportarme su experiencia y conocimiento sobre Seguridad, vista desde campos diferentes (proveedores, ingeniería, instalación, mantenimiento, cliente final, usuarios, etc.) y al que yo también podía aportar los míos.

Con el fin de hacer la Asociación más atractiva y aportar más valor a los socios ¿Qué iniciativas propondrías?

Potenciaría más el uso del foro de la web de AEINSE.

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

NOV
28 al 30

II Edición de SEDEXPO

La feria internacional de Seguridad, Defensa y Emergencias tendrá lugar del 28 al 30 de Noviembre en el recinto Feira Internacional de Galicia Abanca - Silleda (Pontevedra).

En esta edición destaca el carácter dinámico de la exposición, mostrando en funcionamiento multitud de desarrollos y productos. Además se apostará de nuevo por el intercambio de conocimiento y experiencias, la generación negocio, tomar el pulso al mercado y conocer no sólo las novedades de estos ámbitos, sino también las últimas tendencias.

+ información aquí

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

Sicurezza
International Security & fire exhibition

NOV
15 al 17

Entre el 15 y el 17 de noviembre tendrá lugar en Milán una nueva edición de la feria Sicurezza. Como en anteriores ediciones estará ubicada en el recinto Fiera Milano (Rho).

Evento líder en Italia y uno de los más importantes de Europa, **Sicurezza** es un escaparate de novedades y centro de encuentro y debate para todos los actores implicados en las tecnologías de Seguridad y protección contra incendios. Con una amplia área expositiva y una oferta formativa certificada, satisface las necesidades de empresa, asociaciones y profesionales del sector.

+ INFORMACIÓN

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

VI Conferencia sectorial de Seguridad en Puertos

14 NOV 2023

El próximo 14 de noviembre, en la sede de COEM en Madrid, tendrá lugar la VI Conferencia Sectorial de Seguridad en Puertos.

Un evento de carácter bianual organizado por la **Fundación Borredá** en colaboración con **Seguritecnia, Red Seguridad** y **Puertos del Estado**. La conferencia abordará numerosas cuestiones de interés encaminadas a mejorar la protección en el ámbito portuario de la mano de varios expertos tanto del sector público como del privado.

PROGRAMA + INSCRIPCIÓN

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

VI Congreso de Seguridad Privada en Euskadi

08 NOV 2023

El Palacio Euskalduna de Bilbao será el escenario del 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 próximo 8 de noviembre el encuentro reunirá a instituciones, expertos y empresas líderes del sector.

En las ponencias y debates programados se analizarán los avances en seguridad y los desafíos futuros, así como el desarrollo y tendencias en las nuevas tecnologías, destacando la IA y la videovigilancia.

+ INFORMACIÓN E INSCRIPCIÓN

EL INDEPENDIENTE

Economía | Empresas

El apagón del 2G y 3G amenaza con dejar miles de alarmas sin conexión a hogares y empresas en 2024

Las empresas de seguridad siguen aumentando su facturación

CARLOS R. CÓZAR

23/10/23 - 00: 05

Comentar

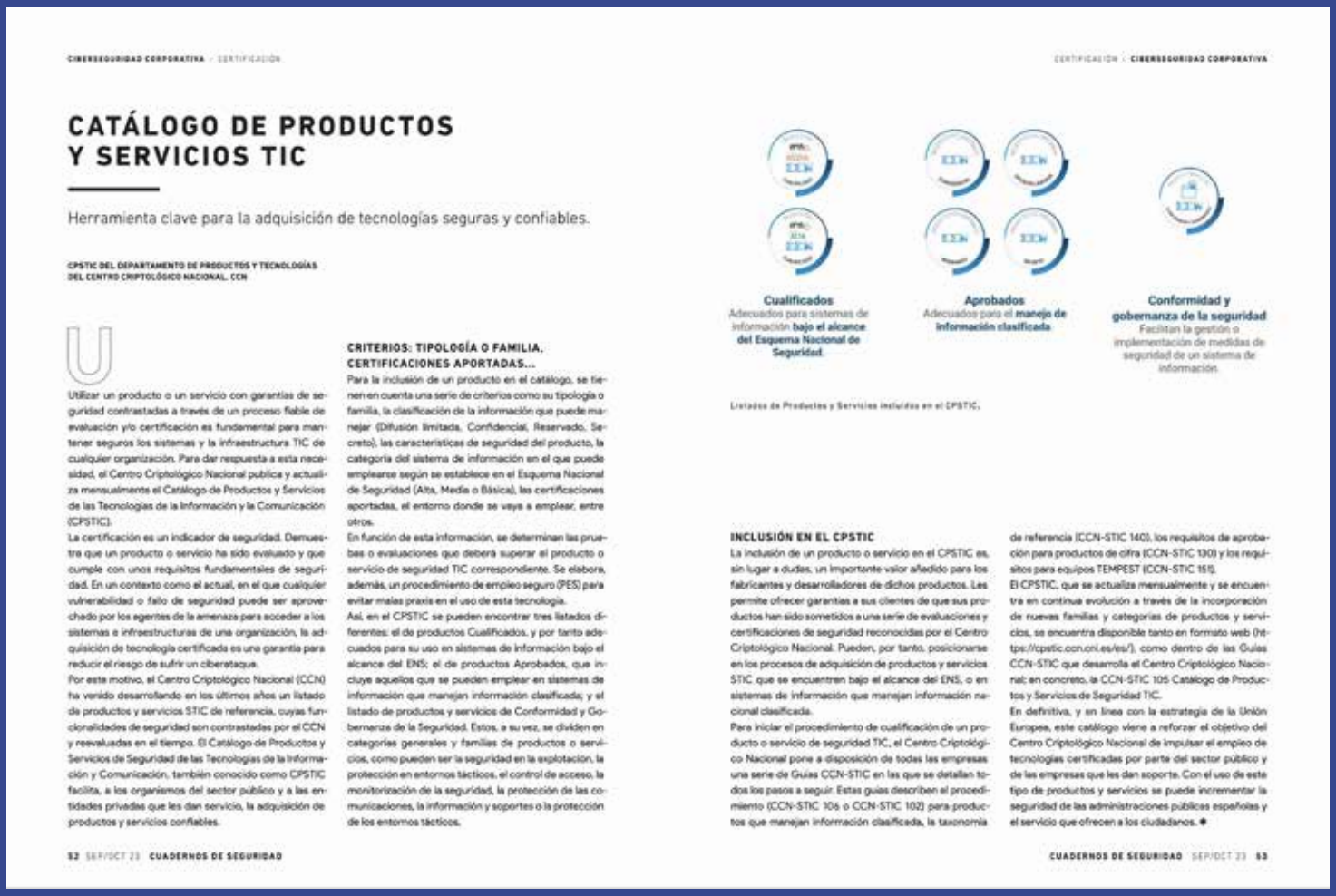
Con la implantación de las **redes 4G** y **5G**, la Unión europea y otras regiones mundiales, decidieron dejar sin servicio las redes 2G y 3G. España es uno de los países en los que este apagado se ha ido retrasando más. Según el artículo *"hay miles de alarmas enganchadas a las redes 2G y 3G y existe cierto retraso en el cambio de tecnología en los aparatos de las alarmas"*.

Por esta razón y otras similares, **Telefónica** y **Vodafone** decidieron postergar el "apagón de las redes". El artículo, en general, no fija fechas concretas. Otras fuentes, como **ADSLzone**, comunican las fechas previstas para el apagado de las empresas proveedoras del servicio; **Movistar, Orange** y **Vodafone**.

+ **información** en:
https://www.elindependiente.com/economia/2023/10/23/el-apagon-del-2g-y-3g-amenaza-con-dejar-miles-de-alarmas-sin-conexion-a-hogares-y-empresas-en-2024/

https://www.adslzone.net/noticias/operadores/apagado-2g-3g-planes-2022/

CUADERNOS DE SEGURIDAD



CIBERSEGURIDAD CORPORATIVA · CERTIFICACIÓN

CATÁLOGO DE PRODUCTOS Y SERVICIOS TIC

Herramienta clave para la adquisición de tecnologías seguras y confiables.

CPSTIC DEL DEPARTAMENTO DE PRODUCTOS Y TECNOLOGÍAS DEL CENTRO CRIPTOLÓGICO NACIONAL. CCN

Utilizar un producto o un servicio con garantías de seguridad contrastadas a través de un proceso fiable de evaluación y/o certificación es fundamental para mantener seguros los sistemas y la infraestructura TIC de cualquier organización. Para dar respuesta a esta necesidad, el Centro Criptológico Nacional publica y actualiza mensualmente el Catálogo de Productos y Servicios de las Tecnologías de la Información y la Comunicación (CPSTIC).

La certificación es un indicador de seguridad. Demuestra que un producto o servicio ha sido evaluado y que cumple con unos requisitos fundamentales de seguridad. En un contexto como el actual, en el que cualquier vulnerabilidad o fallo de seguridad puede ser aprovechado por los agentes de la amenaza para acceder a los sistemas e infraestructuras de una organización, la adquisición de tecnología certificada es una garantía para reducir el riesgo de sufrir un ciberataque.

Por este motivo, el Centro Criptológico Nacional (CCN) ha venido desarrollando en los últimos años un listado de productos y servicios STIC de referencia, cuyas funcionalidades de seguridad son contrastadas por el CCN y reevaluadas en el tiempo. El Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación, también conocido como CPSTIC facilita, a los organismos del sector público y a las entidades privadas que les dan servicio, la adquisición de productos y servicios confiables.

CRITERIOS: TIPOLOGÍA O FAMILIA, CERTIFICACIONES APORTADAS...

Para la inclusión de un producto en el catálogo, se tienen en cuenta una serie de criterios como su tipología o familia, la clasificación de la información que puede manejar (Difusión limitada, Confidencial, Reservado, Secreto), las características de seguridad del producto, la categoría del sistema de información en el que puede emplearse según se establece en el Esquema Nacional de Seguridad (Alta, Media o Básica), las certificaciones aportadas, el entorno donde se vaya a emplear, entre otros.

En función de esta información, se determinan las pruebas o evaluaciones que deberá superar el producto o servicio de seguridad TIC correspondiente. Se elabora, además, un procedimiento de empleo seguro (PES) para evitar malas praxis en el uso de esta tecnología.

Así, en el CPSTIC se pueden encontrar tres listados diferentes: el de productos Cualificados, y por tanto adecuados para su uso en sistemas de información bajo el alcance del ENS; el de productos Aprobados, que incluye aquellos que se pueden emplear en sistemas de información que manejan información clasificada; y el listado de productos y servicios de Conformidad y Gobernanza de la Seguridad. Estos, a su vez, se dividen en categorías generales y familias de productos o servicios, como pueden ser la seguridad en la explotación, la protección en entornos tácticos, el control de acceso, la monitorización de la seguridad, la protección de las comunicaciones, la información y soportes o la protección de los entornos tácticos.

52 SEP/OCT 23 CUADERNOS DE SEGURIDAD

CERTIFICACIÓN · CIBERSEGURIDAD CORPORATIVA

Cualificados
Adecuados para sistemas de información **bajo el alcance del Esquema Nacional de Seguridad**.

Aprobados
Adecuados para el **manejo de información clasificada**.

Conformidad y gobernanza de la seguridad
Facilitan la gestión o implementación de medidas de seguridad de un sistema de información.

Listados de Productos y Servicios incluidos en el CPSTIC.

INCLUSIÓN EN EL CPSTIC

La inclusión de un producto o servicio en el CPSTIC es, sin lugar a dudas, un importante valor añadido para los fabricantes y desarrolladores de dichos productos. Les permite ofrecer garantías a sus clientes de que sus productos han sido sometidos a una serie de evaluaciones y certificaciones de seguridad reconocidas por el Centro Criptológico Nacional. Pueden, por tanto, posicionarse en los procesos de adquisición de productos y servicios STIC que se encuentren bajo el alcance del ENS, o en sistemas de información que manejan información nacional clasificada.

Para iniciar el procedimiento de cualificación de un producto o servicio de seguridad TIC, el Centro Criptológico Nacional pone a disposición de todas las empresas una serie de Guías CCN-STIC en las que se detallan todos los pasos a seguir. Estas guías describen el procedimiento (CCN-STIC 106 o CCN-STIC 102) para productos que manejan información clasificada, la taxonomía de referencia (CCN-STIC 140), los requisitos de aprobación para productos de cifra (CCN-STIC 130) y los requisitos para equipos TEMPEST (CCN-STIC 151).

El CPSTIC, que se actualiza mensualmente y se encuentra en continua evolución a través de la incorporación de nuevas familias y categorías de productos y servicios, se encuentra disponible tanto en formato web (https://cpstic.ccn.cni.es/es/), como dentro de las Guías CCN-STIC que desarrolla el Centro Criptológico Nacional; en concreto, la CCN-STIC 105 Catálogo de Productos y Servicios de Seguridad TIC.

En definitiva, y en línea con la estrategia de la Unión Europea, este catálogo viene a reforzar el objetivo del Centro Criptológico Nacional de impulsar el empleo de tecnologías certificadas por parte del sector público y de las empresas que les dan soporte. Con el uso de este tipo de productos y servicios se puede incrementar la seguridad de las administraciones públicas españolas y el servicio que ofrecen a los ciudadanos. ◆

CUADERNOS DE SEGURIDAD SEP/OCT 23 53

La revista, en la página 52 de su número 372, publica un artículo titulado **Catálogo de Productos y Servicios de la Tecnologías de la Información (CPSTIC)**, destacando el valor de esta herramienta creada por el CCN para facilitar, a los organismos del sector público y a las entidades privadas, la selección de productos y servicios confiables.

Leer el artículo completo **aquí**

• Últimas noticias

El Confidencial
EL DIARIO DE LOS LECTORES INFLUYENTES

Iniciar sesión

MUSTAFA SULEYMAN, COFUNDADOR DE DEEPMIND

Los riesgos de la Inteligencia Artificial

Hubo una época en que la empresa británica DeepMind era el OpenAI del momento. Google la compró, pero su cofundador, Mustafa Suleyman, dejó el buscador decepcionado. Ahora avisa de los riesgos de la inteligencia artificial

En su página web, el diario publica una interesante entrevista a **Mustafá Suleyman**, uno de los cofundadores, en 2010, de **DEEPMIND**, convertida en empresa puntera en IA a nivel mundial y comprada por Google en 2014. En 2022 Suleyman abandonó Google para crear **Inflection AI** con el fin de desarrollar sus propios proyectos: "la búsqueda en el futuro será conversacional, más parecida a un chat que a una lista de enlaces".

Suleyman nos habla del gran futuro de la IA, pero también de los riesgos que conlleva.

Leer el artículo completo **aquí**

Antifrágil

Las cosas que se benefician del desorden

Lo primero que llama la atención es que la palabra no existe en el diccionario de la RAE. Pero el autor, nos da su propia definición *"Algunas cosas se benefician de los sobresaltos, prosperan y crecen cuando se exponen a la volatilidad, la aleatoriedad, el desorden y los factores estresantes y aman la aventura, el riesgo y la incertidumbre.*

Sin embargo, a pesar de la ubicuidad del fenómeno, no hay palabras para lo opuesto a lo frágil, llamémoslo antifrágil. La antifragilidad está más allá de la resiliencia o la solidez. El resiliente resiste los choques y permanece igual, el antifrágil mejora".

A lo largo del libro, **Taleb** indaga en los dominios de lo frágil, lo robusto y lo antifragil, dando claves para medirlo y de cómo obtener beneficios del desorden, el caos y los acontecimientos adversos. Conceptos extrapolables en gran medida al mundo empresarial.

ISBN: 9788449328640

LEÍDO, VISTO Y OÍDO EN...

ISACA

"La victoria por vigilancia no es posible: para ganar hay que enfrentarse al adversario"

Así comienza el artículo de **Scott Fogarty**, director ejecutivo de Ridgeback Network Defense Inc.

"Es una realidad desconcertante que los objetivos empresariales de TI desde los albores de los bytes (hacer que los sistemas sean accesibles, interoperables, ubicuos y, por lo tanto, valiosos) nos hayan llevado a un lugar en el que ahora debemos gastar cientos de miles de millones cada año en ciberseguridad solo para tratar de garantizar que la TI siga siendo un activo y no se transforme en un pasivo".

Ver artículo

PATROCINADORES

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