BOLETÍN Nº60 FEB 2025

AEINSE
Asociación Española de Ingenieros de Seguridad

Congreso y Asamblea´25
en el horizonte...

AEINSE
Asociación Española de Ingenieros de Seguridad

Mensaje de la Junta Directiva

Congreso y Asamblea en el horizonte...

Nos complace anunciar que en breve se celebrará un nuevo Congreso de Ingeniería de Seguridad, el tercero, retomando la senda de los dos primeros que se celebraron antes de la pandemia. Este evento representa una magnífica oportunidad para reunirnos, compartir conocimientos y explorar las últimas innovaciones en el campo de la seguridad.

El congreso contará con ponencias de destacados expertos, que abordarán temas de gran relevancia para nuestra profesión. Entre los temas a tratar se incluyen las tecnologías emergentes en Inteligencia Artificial, la ciberseguridad, etc. Estamos convencidos de que estas presentaciones serán de gran interés y utilidad para todos los asistentes.

Queremos destacar que todos los socios de la asociación tendrán acceso gratuito al congreso. Esta decisión refleja nuestro compromiso de proporcionar a nuestros asociados las mejores oportunidades de formación, desarrollo profesional y networking.

Creemos firmemente que la educación continua y el intercambio de conocimientos son fundamentales para el crecimiento y fortalecimiento de nuestra comunidad.

Además del congreso, el día anterior, celebraremos nuestra Asamblea Anual Ordinaria, cuya fecha se comunicará lo antes posible. Esta reunión es una excelente ocasión para que los miembros participen activamente en la toma de decisiones de la asociación, revisen las actividades realizadas durante el último año y aporten sus ideas y sugerencias para el futuro.

La participación de todos es vital para asegurar que nuestra asociación siga avanzando y adaptándose a los cambios del sector.

Al concluir la asamblea, tendremos el placer de compartir la acostumbrada cena de confraternización. Este será un momento perfecto para fortalecer los lazos entre nosotros, compartir experiencias y disfrutar de una velada agradable en compañía de colegas y amigos.

Para aquellos socios que residan fuera de Madrid, hemos dispuesto cubrir una noche de hotel, asegurando así su comodidad y facilitando su participación en estos eventos tan importantes.

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

LEGIC

NUEVO PATROCINADOR

BIENVENIDA

LEGIC nuevo patrocinador de AEINSE

Damos la bienvenida a nuestro grupo de patrocinadores a LEGIC.

Con más de 30 años en el sector de la seguridad, **LEGIC Identsystems**, con sede en Suiza, ha permitido a empresas de todo el mundo implementar soluciones con exigentes requisitos de seguridad. La tecnología **LEGIC** se basa en módulos de seguridad interoperables que pueden leer todas las normas RFID relevantes a escala mundial, soluciones para la gestión de claves y autorizaciones, y aparte del soporte de identificación, tarjetas a prueba de copias y credenciales móviles seguras para sistemas del control de acceso.

Confiamos en que su presencia en **AEINSE** facilite la comunicación con nuestros socios ingenieros. Desde estas páginas queremos agradecer su apoyo, confianza y colaboración manifestadas hacia nuestra Asociación.

+INFORMACIÓN

AEINSE
Asociación Española de Ingenieros de Seguridad

NOTICIAS AEINSE

GRUPO DE TRABAJO DE
BUENAS PRÁCTICAS

"Guía de buenas prácticas de gestión y mantenimiento de la ciberseguridad en sistemas de seguridad física"

GRUPO DE TRABAJO DE **CIBERSEGURIDAD**

El Grupo se encuentra analizando cómo nuestro documento ya redactado **"Guía de buenas prácticas de gestión y mantenimiento de la ciberseguridad en sistemas de seguridad física"** se complementa con la reciente publicación del Foro Nacional de Ciberseguridad **"La gestión de la ciberseguridad de los sistemas de seguridad física"**, recogiendo algunos de los aspectos incorporados en ella.

El documento del Foro, con su enfoque analítico, casos de uso y evaluación de ciberriesgos, aporta una visión táctica que podría fortalecer las prácticas descritas en **AEINSE.** En particular, el análisis de amenazas y salvaguardas del Foro podría enriquecer las políticas internas y estrategias de mejora continua de **AEINSE**, ayudando a alinear su enfoque operativo con escenarios reales y riesgos concretos.

SCATI revoluciona la seguridad con interconexión y eficiencia

SCATI, fabricante de soluciones inteligentes de seguridad, organizó el pasado 6 de febrero en Madrid el evento "Evoluciona la Seguridad de tu Infraestructura: Interconexión y Eficiencia Operativa", donde presentó SCATI SENTRY, su innovadora plataforma de integración de sistemas, reconocida como Mejor Producto de Seguridad 2024 por la revista Seguritecnia, consolidando su liderazgo en el sector.

El evento reunió a expertos del sector para analizar el impacto de la tecnología en la seguridad. **Alfonso Mata**, CEO de SCATI, destacó la transformación digital como eje central del futuro de la seguridad. **Sergio Gómez**, R&D Director, presentó **SCATI SENTRY**, plataforma clave para la gestión integral de infraestructuras, y **Beatriz Vielva** realizó una demostración en vivo, destacando su funcionalidad y beneficios.

La mesa de debate, con líderes de seguridad de **Naturgy, Cellnex** y **Logista,** abordó retos clave como la regulación de la biometría, la formación de técnicos, la inteligencia artificial y la importancia del factor humano en situaciones de crisis resaltando su papel insustituible en la toma de decisiones críticas.

Los asistentes pudieron experimentar de primera mano el potencial de **SCATI SENTRY** en la Zona de Experiencia Interactiva, comprobando su capacidad para optimizar la seguridad y eficiencia operativa de infraestructuras.

+información

AXIS COMMUNICATIONS

Axis presenta la próxima generación de captura de imágenes análisis potenciados por IA y ciberseguridad con el

SoC ARTPEC-9

Axis anuncia la 9ª generación de su sistema en chip (SoC) de diseño propio. ARTPEC-9 utiliza y perfecciona las capacidades y funciones que caracterizan a las generaciones anteriores del SoC de diseño propio de la empresa:

- **Velocidad de bits excepcionalmente baja**
- **Análisis potenciado por IA**
- **Imágenes de calidad**
- **Ciberseguridad mejorada**

La ciberseguridad es el núcleo del diseño de ARTPEC-9. Características como el arranque seguro y el sistema operativo firmado garantizan que cada dispositivo permanezca protegido de las ciberamenazas. Además, dado que ARTPEC-9 se desarrolla internamente, Axis conserva el control total sobre el proceso de producción, lo que refuerza aún más la seguridad del dispositivo.

Además, por primera vez en grabaciones de vídeo en red, ARTPEC-9 es compatible con el probado estándar de codificación de vídeo AV1 de la Alliance for Open Media (AOM). Junto con Axis Zipstream, AV1 facilita la reducción del coste de almacenamiento sin sacrificar el más mínimo detalle.

+información

IVA Pro Privacy

máscaras de privacidad para objetos en movimiento

BOSCH

La nueva máscara de privacidad dinámica de Bosch pixela a personas y vehículos en la propia cámara (Edge).

El proceso de legalización de los sistemas de videovigilancia está asociado al uso que se prevé hacer de las imágenes. La vigilancia del tráfico, la protección de un edificio, o la seguridad ciudadana, requieren de autorizaciones diferentes, todas ellas relacionadas con la protección de los datos personales.

Son especialmente sensibles los sistemas de videovigilancia instalados en la vía pública por las Fuerzas y Cuerpos de Seguridad, ya que en estos casos la seguridad prevalece sobre la privacidad, por lo que es un tribunal de justicia el que aprueba su implantación.

En este escenario, disponer de una herramienta que permita enmascarar a las personas, manteniendo su anonimato, es clave para el éxito de proyectos relacionados con la protección de eventos en la vía pública, el análisis de los flujos peatonales en zonas comerciales o turísticas, o el control de aforo en espacios de alta ocupación.

IVA Pro Privacy ofrece la posibilidad de enmascarar la imagen de la cámara total o parcialmente, la persona al completo o solo el rostro, y, a la vez, permite aplicar otras analíticas en estas zonas con el fin de obtener metadatos anonimizados, estadísticas, y eventos de alarma. **IVA Pro Privacy** se aplica en la cámara, garantizando que no existe tratamiento de imágenes sin anonimizar fuera del dispositivo.

Profundiza en el sector de la seguridad con la Academia Casmar

La seguridad evoluciona, y con ella, los profesionales que lideran el sector. La Academia Casmar nació para que quienes quieran ampliar sus conocimientos reciban la mejor formación posible. Por ello, hemos diseñado cursos especializados de electrónica de red cibersegura, formación para pilotos de drones y la certificación de Vigiplus (Desico).

Además de nuestros programas actuales, estamos orgullosos de presentar nuestro nuevo curso de seguridad básica, dirigido a aquellos que desean fortalecer sus fundamentos y comenzar una carrera en este campo esencial.

Aprende de expertos con amplia experiencia en la industria y accede a formación diseñada para que realmente entiendas y apliques los conocimientos de manera práctica. Nuestros cursos te prepararán para enfrentar los desafíos reales de la seguridad en entornos tecnológicos.

Si quieres ampliar tus conocimientos en seguridad, aquí encontrarás cursos adaptados a tu nivel y necesidades.

Invierte en tu futuro con formación de calidad y conviértete en un referente en el sector de la seguridad.

Consulta nuestros cursos y fórmate con los mejores:

+información

dormakaba

En el mundo de la seguridad y el acceso inteligente, dormakaba pone en al mercado su tecnología TouchGo que puede ser integrada, entre otros dispositivos, en la cerradura electrónica c-lever pro. Este sistema permite a los usuarios abrir puertas sin necesidad de utilizar llaves o tarjetas de proximidad, simplemente tocando la maneta con la mano.

c-lever pro TouchGo

la revolución del acceso inteligente sin contacto

La tecnología **Resistive Capacitive Identification Device (RCID)** reconoce la presencia de un medio físico de usuario autorizado en un radio cercano, ofreciendo una experiencia de acceso mas cómoda ideal para entornos de alta seguridad y flujo constante de personas. **C-lever pro TouchGo**, combina **RCID** y **RFID** para integrarse en los ecosistemas **dormakaba KEM, MATRIX**, etc.

Entre sus principales beneficios se destacan:

- **Facilidad de uso:** basta con tocar la manija para desbloquear la puerta.
- **Mayor higiene:** se reduce el contacto con superficies comunes al eliminar la necesidad de llaves.
- **Programación flexible:** los administradores pueden gestionar accesos de manera sencilla a través de listas blancas manuales o software de sistema.
- **Modos adicionales:** incluye Office Mode y Pass Mode, que permiten mantener la puerta abierta según las necesidades del entorno.
- **Bajo mantenimiento:** gracias a su diseño eficiente, las baterías tienen una larga duración y pueden sustituirse con facilidad.
- **Versatilidad:** su diseño moderno y resistente lo hace ideal para oficinas, hospitales, hoteles y espacios comerciales.

TouchGo de **dormakaba** es la solución perfecta para espacios que buscan combinar seguridad, innovación y comodidad en un solo dispositivo.

¡Descubre una nueva forma de acceso inteligente y simplifica tu vida diaria!

+información

Ciberesistencia
principal tendencia de 2025

En un entorno digital en constante evolución, las amenazas cibernéticas han escalado en complejidad y alcance, poniendo en riesgo a empresas de todos los sectores, especialmente aquellas consideradas críticas para el funcionamiento de la sociedad. Para reforzar la seguridad de estas entidades, la Unión Europea ha implementado la directiva NIS2, un marco legislativo que busca estandarizar y mejorar la ciberseguridad en toda la región, obligando a las organizaciones críticas y esenciales a elevar sus estándares de seguridad.

En este contexto, empresas como **DORLET®**, que desde hace años integran la ciberseguridad en su ADN, están bien posicionadas para adaptarse rápidamente a los nuevos requisitos. Sus soluciones, certificadas por organismos oficiales como la Agence Nationale de la Sécurité des Systèmes d'Information - ANSSI (certificación CSPN), y su cumplimiento con estándares como el RGPD, ISO 27001 y el Esquema Nacional de Seguridad, reflejan un compromiso sólido con la seguridad física y digital.

Aunque la NIS2 supone una oportunidad para revisar y optimizar estrategias, expertos del sector coinciden en que compañías que han estado haciendo los deberes hasta la fecha, como **DORLET®**, tan solo tendrán que hacer unos pequeños ajustes y revisar su estrategia, pero no supondrá un rompecabezas para ellas ni para sus clientes.

En cualquier caso, en **DORLET®** seguiremos trabajando para estar a la vanguardia de la seguridad y proteger a nuestros clientes de amenazas físicas y cibernéticas, tanto actuales como futuras.

VIDEOSISTEMAS FFV GEUTEBRÜCK

F.F. Videosistemas

innova con soluciones de vídeo para diferentes sectores

Gracias a los nuevos dispositivos con inteligencia artificial, desarrollamos nuevas herramientas para simplificar la gestión de las instalaciones más complejas.

Sistemas de grabación G-CORE

La última tecnología alemana aplicada al sector de la seguridad.

Sistemas con protección de datos basada en las medidas más estrictas de ciberseguridad. Hardware industrial con la máxima fiabilidad para instalaciones con necesidades de alta disponibilidad.

+información

Software de gestión G-SIM

Plataforma de gestión de vídeo y datos para la optimización de procesos.

Capacidad de auditoría de usuarios, planimetría, redundancia, gestión avanzada de alarma, gestión de eventos y metadatos.

+información

PNS-NEXUS

Plataforma de gestión de eventos aplicable a diferentes sectores.

Gestión de matrículas para entornos de control de accesos, instalaciones logísticas y ciudades inteligentes. Herramienta de trazabilidad de códigos basada en imágenes para departamentos de operaciones del sector logístico. Búsquedas para análisis forense basadas en atributos de objetos (personas y vehículos).

+información

Cámaras entrenadas con IA

Última generación de cámaras entrenadas con inteligencia artificial que mejoran la precisión de detección de intrusiones y la monitorización de objetos.

Generan canales de eventos de analítica para reducir la carga de trabajo de los centros de control.

+información

Hanwha Vision

Hanwha Vision

lanza Wisenet Access Control System

Hanwha Vision ha lanzado Wisenet Access Control System, una solución de control de acceso integrado con videovigilancia, para una gestión de seguridad más eficiente y completa.

Wisenet Access Control System se integra con los sistemas de gestión de video Wisenet Wave y SSM, ofreciendo una plataforma única para controlar y supervisar accesos en tiempo real.

- **Gestión remota y visualización en vivo:** A través de Wave o su app, los operadores pueden administrar accesos y ver imágenes en directo, para una mejor supervisión.
- **Información clave:** Wave muestra en pantalla, sobre la imagen de la cámara, datos como hora y ubicación del acceso.
- **Registro de eventos críticos:** Los operadores pueden marcar y guardar incidentes relevantes, como accesos no autorizados o puertas forzadas, para analizarlos posteriormente.

El sistema ofrece una amplia gama de funciones que garantizan la seguridad de su empresa:

- **Gestión integral de puertas:** Para situaciones de emergencia o incidentes de seguridad.
- **Flexibilidad:** Permite el control de dispositivos de terceros
- **Interlocking:** Diseñado para entornos de alta seguridad (esclusas).
- **Anti-Passback:** Accesos no autorizados al impedir que los usuarios compartan tarjetas.
- **Control de acceso a ascensores.**
- **Accesos con doble autenticación.**

El sistema ofrece distintas opciones de licencias según las necesidades de cada negocio:

- **Lite:** Hasta 6 puertas.
- **Estándar:** Hasta 32 puertas.
- **Profesional:** Hasta 256 puertas.
- **Empresarial:** Sin límite de puertas

+información

Johnson Controls

Innovación en Videovigilancia

Cámaras Illustra Flex y Pro de Johnson Controls con Inteligencia Artificial

La gama de cámaras Illustra Flex y Pro integran funcionalidades diferenciadoras de Inteligencia Artificial (IA). Estas cámaras son capaces de categorizar objetos como personas, coches, camiones, motocicletas, mochilas, maletas entre otros objetos, facilitando una identificación precisa en tiempo real.

Un aspecto destacado es la capacidad de identificar los colores de las prendas de ropa de las personas y de los vehículos, lo que permite una búsqueda más efectiva en situaciones críticas. Además, la creación de reglas combinadas con analítica en cámara, como el cruce de línea, merodeo y detección de objetos abandonados, automatiza la respuesta a los eventos, enfocándose en lo que realmente importa.

Las cámaras Illustra también mejoran la exposición de las imágenes, garantizando que las imágenes de las personas detectadas por IA sean de la mejor calidad.

Además para preservar la privacidad, generan máscaras dinámicas sobre las personas detectadas, ayudando en el cumplimiento de las normativas de protección de datos allí donde sea requerido.

Equipadas con un chip dedicado para el procesamiento de IA y los más altos niveles de ciberseguridad, no requieren hardware adicional, lo que optimiza su implementación. En conjunto, estas características no solo aumentan la precisión y eficiencia en la vigilancia, sino que también proporcionan información valiosa para la investigación forense, mejorando significativamente el rendimiento del equipo de seguridad.

+información

Lanaccess obtiene la certificación ISO 27001

La ISO 27001 es el estándar internacional más riguroso para la gestión de la ciberseguridad.

Numerosas auditorías externas han evaluado las políticas corporativas de Lanaccess, así como los procedimientos y la tecnología desarrollada en su centro de I+D+i. Esta tecnología incluye los equipos de videovigilancia y de software (firmware de los equipos, el VMS y la analítica avanzada).

La certificación se extiende a su sede central en Barcelona y a sus oficinas estratégicas en Madrid y Ciudad de México.

Emitida por **Staunchly Management And System Services Ltd.**, con auditoría de Iscertia, esta certificación refuerza el compromiso de **Lanaccess** con la protección de los datos en un entorno dinámico.

Además, se alinea con normativas internacionales clave con las que ya cuenta el fabricante, como la **NDAA, NIS 2, DORA** y el **RGPD.**

La **ISO 27001** consolida a **Lanaccess** como un fabricante líder y confiable en la industria de la videovigilancia.

+información

AEINSE
Asociación Española de Ingenieros de Seguridad

LEGIC

NOTICIAS
PATROCINADORES

SEGURIDAD EN LAS CREDENCIALES DE LOS SISTEMAS DE CONTROL DE ACCESO:

Seguridad por diseño con la solución de encriptación y gestión de autorizaciones

"Master-Token-System-Control" (MTSC) de LEGIC

Para garantizar la seguridad integral de un sistema de control de acceso, es esencial que el sistema utilizado se base en un diseño seguro. Un aspecto clave es la transmisión cifrada de datos entre el lector (que puede ser mural o estar intregrado en cilindros electrónicos, lectores murales o cerraduras de armario) y los soportes de datos (tarjetas RFID, llaveros o smartphones), para evitar que los datos sensibles sean interceptados y/o copiados.

No especificar la tecnología utilizada para cifrar la información de la credencial en la comunicación entre los soportes de datos y los lectores puede significar una vulnerabilidad relevante en el sistema de seguridad.

Se recomienda utilizar únicamente soluciones RFID con tecnología de 13,56 MHz, que ofrezcan al menos un cifrado AES de 128 bits. Esto incluye advant, el estándar RFID de **LEGIC**, que puede adquirirse junto con el **MTSC "Master-Token-System-Control"**. El propietario de un **MTSC** recibe de **LEGIC** una tarjeta física con su material de llave de cifrado individual, que puede transferirse a los lectores y a los medios de identificación, a prueba de escuchas y copias.

Por lo tanto, el propietario del **MTSC** controla su propia llave de cifrado y es independiente de los proveedores de componentes.

Para grandes aplicaciones, el sistema **MTSC** permite establecer una jerarquía de autorizaciones individual, por ejemplo, por país, ubicación, departamento, aplicación, etc. El **MTSC** permite, solo a la persona autorizada, el poder de generar, distribuir o revocar autorizaciones basadas en su llave de cifrado en cualquier momento y de forma auditable.

+información

Solución Avanzada en Seguridad y Vigilancia

QVMS LiDAR Video Analytics

Sicuralia presenta QVMS LiDAR Video Analytics (VA), una solución avanzada de video-análisis en tiempo real para sensores LiDAR y cámaras de CCTV. Diseñada para optimizar la seguridad y vigilancia en entornos profesionales, está totalmente integrada con el sistema de gestión de video Qognify QVMS. QVMS VA ofrece un factor de fiabilidad adicional, utilizando los datos obtenidos de los sensores LiDAR para detectar la forma y posición exacta de los intrusos en escenarios 3D.

Entre sus capacidades clave, **QVMS VA** incluye:

- **Detección por láser 3D:**
  Detección 3D a través de sensores laser LiDAR
- **Detección por video:**
  Video detección en tiempo real.
- **Protección perimetral:**
  Detección de intrusos y análisis de movimiento.
- **Anonimidad intrínseca:**
  Las detecciones generadas por los LiDAR no muestran identidad.
- **Detección de incendios y humo:**
  Con una calibración avanzada para mayor precisión.

QVMS VA complementa los sistemas de detección perimetral físicos, con sensores **LiDAR 3D** y cámaras de video-vigilancia monitorizadas a través de **Hexagon Qognify QVMS.**

La integración de sensores físicos y videoanálisis en una única plataforma proporciona una solución de seguridad robusta, ideal para instalaciones con altas exigencias de protección, donde la privacidad es un factor importante.

+información

ATENDER EMERGENCIAS DEL SIGLO XXI

CON TECNOLOGÍA ANTERIOR A EDISON

Rafael
Moro Fonseca

Vicepresidente de la Asociación Española
de Lucha Contra el Fuego

¿SE IMAGINAN QUE DE REPENTE NO FUNCIONASE LA TELEFONÍA MÓVIL, NI EL RESTO DE SISTEMAS DE COMUNICACIÓN, LOS VEHÍCULOS FABRICADOS CON POSTERIORIDAD A LOS AÑOS 90 SE PARASEN, LOS EQUIPOS QUE FUNCIONAN CON ELECTRÓNICA FALLARAN; NO DISPUSIÉRAMOS DE ELECTRICIDAD...?

Pues los expertos en el estudio de las denominadas "tormentas solares", auguran que todo eso ocurrirá en el 2025, en una parte del mundo, como consecuencia de la afectación a la tierra de uno de tales eventos.

¿Ciencia ficción?

No debía serlo para Barack Obama, quien, poco antes de cesar en su cargo de Presidente de Estados Unidos, firmo una "orden ejecutiva", dirigida a Secretarías y Agencias del gobierno, para que desarrollasen un plan de actuación, haciendo especial hincapié en el apagado manual de las centrales atómicas, si se producían eventos climáticos espaciales, como las tormentas solares.

Ni para los canadienses que, el 12 de marzo de1989, se enfrentaron a las consecuencias, narradas al principio de este artículo, provocadas por una de esas tormentas.

En las siguientes páginas, se va a tratar sobre tormentas.

Aunque se trate de unas muy peculiares, porque son producidas por el Sol, han de considerarse, en lo que se refiere a sus características y evolución, como un fenómeno natural más.

Pues parece claro que a la mayoría de las personas nos resulta interesante, cuando no conveniente, conocer el "tiempo meteorológico" que va hacer en la zona donde vamos a desarrollar alguna actividad; pues esa información va a influir en nuestra conducta y vestimenta a lo largo de las siguientes horas o días.

De hecho, el "tiempo meteorológico", es una conversación habitual cuando entre dos personas, que forzosamente van a compartir espacio temporal y físico, no tienen nada que decirse. Indudablemente, no es lo mismo llevar a cabo una tarea al aire libre si llueve, nieva, se están produciendo tormentas eléctricas, luce un sol intenso, hace calor, hace frío...

Y sin embargo no nos preocupa conocer el estado del sol y como puede afectarnos este estado. Incluso cuando está demostrado que puede causarnos emergencias catastróficas. Porque el sol interacciona con todos los objetos del Sistema Solar y ello genera diversos fenómenos, que guardan relación con lo que vendrían a ser el equivalente a nuestras cuatro "estaciones", pero que en el caso que nos ocupa, denominamos ciclos solares, que se repiten cada once años aproximadamente.

La descripción de las variaciones que esos ciclos producen en el ámbito del universo existente entre el sol y la tierra, forma parte de lo que se denomina "tiempo espacial".

Meteorología espacial

La Meteorología espacial, como la define la Organización Meteorológica Mundial, consiste en: "El análisis del estado físico y fenomenológico del entorno espacial natural, en particular el sol y los entornos interplanetarios y planetarios".

Seguro que leído este texto, quienes tienen competencias en la gestión de emergencias, además de preocuparse por las incidencias que pueden producirse en su trabajo por causa de los fenómenos meteorológicos tradicionales, buscarán información para saber si durante las siguientes horas o días deben temer, como el famoso galo Asterix, que "el cielo caiga sobre su cabeza".

Parece interesante, para empezar a hablar del asunto, conocer cuáles han sido las tormentas solares más importantes, a partir de que la observación científica y la tecnología han permitido diagnosticar el evento "tormenta solar" desde el punto de vista de los daños causados.

Entre el 10 y el 12 de mayo de 2024, una intensa ráfaga de viento solar que llegó a la Tierra desencadenó la migración de la mitad de todos los satélites activos en la de denominada órbita terrestre baja (en ella se encuentran dos estaciones espaciales; miles de satélites con funciones científicas o de comunicaciones y posicionamiento: GPS; GLONAAS, BDS y Galileo...).

Inutilizados los sistemas anticolisión de esos satélites, podríamos habernos visto inmersos en el primer "evento Kessler" (reacción en cadena producida por la colisión de fragmentos de desechos que ya se encuentran en el espacio). Lo que hubiera supuesto una catástrofe tecnológica..., como mínimo.

Pero además, se produjeron alteraciones en infraestructuras de suministro de energía, en zonas del norte de Europa, de Canadá.....

Científicos estadounidenses del Instituto Tecnológico de Massachusetts (MIT) y otros expertos piensan que la situación puede volver a producirse en 2025, al encontrarse el Sol en fase de muy alta actividad.

Un inciso... sólo hay una parte agradable en una tormenta solar: las auroras boreales

Habría que remontarse a los últimos días de octubre del 2003, para encontrarnos con una situación más crítica, provocada por varias de estas tormentas. Satélites y comunicaciones se vieron afectados. Vuelos cuya ruta pasaba por las regiones polares fueron desviados. Incluso en Sudáfrica, doce grandes transformadores fueron

dañados de gravedad.
En julio de 2000 se produce la tormenta de "el Día de La Bastilla", así llamada por coincidir con esta festividad francesa. No produjo grandes daños, pero sirvió para poner a prueba los satélites y sistemas de detección y análisis que fueron lanzados e instalados a partir de 1989 para monitorear al Sol. Año, en el que, como ya se ha escrito en párrafos anteriores, se produjo la más conocida y que provocó el denominado apagón de Quebec.

Si seguimos retrocediendo en el tiempo, nos encontramos, por contra, con la más desconocida: la de mayo de 1921, que afectó a varios estados del norte de USA y seis provincias canadienses. Obviamente, los daños producidos, estaban circunscritos a la tecnología de la época: trenes parados; apagón de luces en calles y edificios; fallos de la red de telegrafía. Pero en todo caso, esta tormenta ha sido la más "potente" sufrida por la Tierra, desde el evento Carrington, así llamado por ser el apellido del científico que detectó la actividad solar el 28 de agosto de 1859.Y que alcanzó a observarse incluso en el sur de España.Ha sido el evento más violento desde que se inician registros de los efectos de las tormentas solares.

La incipiente tecnología, hizo que los daños se limitasen a las redes telegráficas de USA y Europa, que estuvieron inutilizadas mucho tiempo. Pero de sufrirse un evento similar en la actualidad, esos daños, supondrían, en gran parte del mundo, la paralización de las comunicaciones a distancia (incluyendo las realizadas vía cable submarino), imposibilitarían el suministro de electricidad en grandes zonas geográficas y la destrucción de satélites sería masiva. Pudiendo ocasionarse el ya mencionado síndrome de Kessler.

Evento Miyake

Aunque todo puede ser peor, si lo que se manifiesta es el evento Miyake, que podría producir tormentas solares extremas, varias veces más intensas que las que provocó el evento Carrington. Desaparecería la civilización tal y como la conocemos y se perderían millones de vidas. Se tiene conocimiento de su existencia, gracias a los anillos de los troncos de los árboles antiguos, por la gran cantidad de radio carbono 14 concentrada en los que se formaron coincidiendo con este evento. Con ello se ha conseguido saber que se han producido seis de ellos, en los últimos 14.500 años. El más próximo a nosotros en el año 993.

En todo caso, el impacto de las tormentas sobre la tierra sigue un mismo patrón para eventos importantes:

- Primero se produce la erupción de una radiación de alta energía (rayos X y de ultravioleta extremo) que puede afectar a nuestra ionosfera en ocho minutos porque viaja a la velocidad de la luz y cuya duración puede contabilizarse en minutos/horas. Tiempo durante el que se ven muy afectadas, con un alto nivel de ruido (Tormenta de ruido), la banda de HF. Y las redes de geolocalización.

- Le sigue una Tormenta de radiación solar generada por partículas muy cargadas. Esta radiación puede llegar a la tierra, entre 15 minutos y varias horas, después del inicio del evento y su duración puede contabilizare en horas/días.

- Y por último, se generan en el sol eyecciones de masa coronal, que provocan una Tormenta geomagnética, que tarda en afectarnos, produciendo grandes anomalías en el campo magnético terrestre, entre uno y cuatro días, con una duración del efecto, de entre unas horas a varios días.

La intensidad de estas tormentas varía según la latitud. Suelen ser más fuertes en zonas cercanas a los polos. Pero su influencia tiene un carácter global, comenzando simultáneamente en todos los puntos de la Tierra. No obstante, las amplitudes con que se observan en distintos lugares son diferentes, siendo mayores cuanto más altas son las latitudes.

Esperando que lo breve del texto, no impida que se haya entendido qué son las tormentas solares y como afectan a nuestro mundo, voy a comentar, sucintamente, aspectos importantes de la gestión de las emergencias, bajo la influencia de un evento solar. Hay que tener en cuenta, que las telecomunicaciones pueden fallar. Por lo que se debe disponer de sistemas alternativos a las redes de radio y telefonía principales. Pensando incluso en utilizar mensajeros en bicicleta. Filípides no disponía de esa máquina. Los coches modernos, llevan mucha electrónica, por lo que pueden quedarse parados en una tormenta solar. Disponer de algún vehículo, mejor diesel, de antes de los años 90 (sin centralitas) puede facilitar el mando y control de la emergencia.

Pueden producirse problemas de suministro eléctrico, en instalaciones indispensables, como el CECOP (Centro de Coordinación Operativa), CECOPI (Centro de Coordinación Operativa Integrado), PMA (Puesto de Mando Avanzado), etc. Debe contarse, por ello, con generadores diesel, con arranque desde la batería. Y con motobombas, diesel, para trasvase de ese combustible y de agua.

Conclusión

En todo caso, los **Servicios de Atención a las Emergencias**, deben plantearse que tienen que disponer de protocolos de funcionamiento bajo los efectos mencionados... y entrenarlos. Porque, como ocurre con las meigas, puede que no creas que vayas a sufrir un evento solar de gran magnitud, pero, como ha quedado demostrado: "haberlos haylos".

CONOCE A UN

SOCIO

Antonio León González

SOCIO Nº 170
9323alg@gmail.com

Buenas tardes Antonio, para comenzar preséntate a todos nuestros compañeros por favor.

Mi nombre es Antonio León González, soy Ingeniero Técnico Industrial en la especialidad de Electrónica, en la Universidad de Málaga, de la promoción de 2004.

Toda mi carrera profesional, desde 2004 que me diplomé, ha sido en el sector de la seguridad, primero en la parte de Sistemas de Seguridad en todos sus campos: Intrusión, CCTV, CCAA, PCI, CRA, Integración, etc. en todo tipo de instalaciones, empezando más por el tema doméstico y terminando en grandes instalaciones como Hospitales, Maxam o ITP.

Luego, a partir de 2011 mi dedicación ha estado más centrada en las licitaciones del sector de Vigilancia de Seguridad Privada, dejando Málaga y trasladándome al Norte. Actualmente combino la labor de las licitaciones con funciones de gestión y controller en una empresa internacional como I-SEC.

Hace tiempo que eres socio de AEINSE ¿Qué razones te llevaron a asociarte?

Lo primero, que creo que en nuestro sector faltaba profesionalizar nuestra actividad, sobre todo porque hay muy poca o nula formación oficial al respecto, y creo que este tipo de asociaciones ayudan a ello, además de que conocía profesionalmente a las personas que iniciaron este proyecto y ya sabía que sería bueno.

¿Cuál es tu formación académica?

Ingeniero Técnico Industrial en la especialidad de Electrónica, en la Universidad de Málaga.

¿En qué empresas te has desarrollado profesionalmente y con qué responsabilidades?

A las 2 semanas de terminar la carrera, ya empecé en el sector:

- **2004-2006** en la empresa ROJIPER, una empresa de sistemas de seguridad y CRA propia que trabajaba en Málaga:

  En un primer periodo me estuve formando con los técnicos, aprendiendo con funcionaban los sistemas electrónicos de seguridad: alarmas, CCTV, CCAA, etc así como la CRA. Luego pasé a ser el Ingeniero de la empresa.

- **2006-2020** en la empresa PROSETECNISA, una empresa de seguridad integral, con vigilancia, sistemas de seguridad y CRA propia que trabajaba en todo el territorio nacional:

  En un primer periodo me estuve formando con los técnicos, ya que esta empresa trabajaba con una tecnología de sistemas más avanzada que de la que yo venía, especialmente en software de integración, grandes instalaciones de PCI, etc.

  Principalmente empecé en todos los sistemas de los Hospitales de Málaga, y también en otras grandes instalaciones como depósitos de explosivos de Maxam, donde ya se usaban sistemas tan especiales como las barreras de microondas o los GPS de detección de pisadas...

  Luego pasé a ser el responsable de sistemas en la zona de Andalucía y posteriormente a ser el Ingeniero a nivel nacional de la empresa. El fuerte de esta empresa era la vigilancia, y el delegado de Málaga, en un momento dado, me pidió ayuda para preparar licitaciones de vigilancia en Andalucía, empecé poco a poco a ayudarlo, y posteriormente ya me empecé a encargar de realizarlas completamente.

  En el año 2011, el presidente de la empresa me ofreció irme a la central en Barakaldo para encargarme de las licitaciones de vigilancia de la empresa a nivel nacional y acepté, y estuve allí hasta 2020.

  En este tiempo, además de las licitaciones, empecé a trabajar ayudando en labores de Controller de la empresa (análisis de rentabilidades de servicios, etc.), aprendí mucho de la persona con la que trabajaba y eso me ayudó mucho en el análisis de datos.

- **2020-2021** tras 15 años en PROSETECNISA, y debido a la futura venta de la empresa y que me llegó una propuesta de INVICO, decido dar el salto a otra empresa, cuya matriz principal estaba dedicada a RSU y Limpieza, y me llaman para poner en marcha un departamento de proyectos en ambas empresas.

  Los resultado de las licitaciones fueron buenos, pero debido a no estar del todo contento en el funcionamiento de las empresas, decido volver a cambiar tras la propuesta de I-SEC.

- **2021-Actualidad** estoy en I-SEC, empecé como la persona encargada de las licitaciones y actualmente soy el director de Desarrollo de Negocio y Controller de la empresa. En este tiempo la empresa ha crecido mucho, pasando de apenas 700 trabajadores a más de 3000, debido a eso hemos parado un poco en la preparación de licitaciones para centrarnos más en la gestión y control del negocio, y ahí, debido a mi experiencia anterior he pasado de dedicarme sólo a las licitaciones, a más labor de Controller en la empresa.

Comenzaste y continúas en el sector de la seguridad. ¿Qué ves en él para que te resulte atractivo?

La verdad que es una pregunta que no es fácil de contestar, es verdad que empecé en la parte de la seguridad de Sistemas, por mi perfil, pero con el tiempo he ido abandonando esta parte y estar más relacionado con la parte de Vigilancia, que pienso que es bastante menos atractiva para un perfil como el nuestro.

Lo que pasa, es que con el paso del tiempo y la experiencia me siento bastante cómodo en la labor que realizo, cuando ganas una licitación o consigues arreglar un problema en la empresa desde la labor de controller, pues son estímulos y alegrías que te hacen sentir que tu trabajo da sus frutos.

Pero, en sí, creo que el sector de la vigilancia de seguridad necesita cambiar para hacerlo más atractivo en el futuro.

Tienes una gran experiencia en la preparación de licitaciones a nivel nacional. ¿Es muy diferente la preparación y gestión de las mismas en el sector público y el privado?

En este sentido, creo que la mayor diferencia es la oportunidad. En el sector público, es muy fácil concurrir y tener la oportunidad de presentarte a las licitaciones, sin embargo, en el sector privado, creo que la mayor dificultad es que te den la oportunidad de presentar ofertas, y en mi caso, en una empresa como la actual, con poco tiempo en España, es más difícil poder acceder. Pero en sí, la preparación en ambos sectores, es parecida.

Como ayuda a la realización de las licitaciones y propiciar su adjudicación, me consta que desarrollaste un sistema de comparación con la competencia que te permite simular las puntaciones a obtener en el estudio comparativo. ¿En qué consistía este comparador?

Cuando llevamos ya muchos años en el sector y preparando licitaciones, y estás en todo el proceso, pues vas conociendo más o menos los márgenes en los que nos movemos las empresas.

Con la ayuda de la experiencia de manejo de datos en mis labores de Controller, pues empecé a recopilar los datos de las aperturas, comparando nuestros márgenes ofertados, con las demás ofertas y analizando en que márgenes exactos se mueven las demás empresas de la competencia.

Cuando presentas una oferta a una licitación, con la experiencia, depende de para dónde sea la licitación y los criterios, intuyes qué empresas se pueden presentar, sabes más o menos cuales van a ser las ofertas más bajas y altas, y aplicando las fórmulas de los criterios, pues analizamos aproximadamente cual va a ser nuestra puntuación económica respecto a las demás empresas.

Para ello, es importante analizar esta información en función de la fórmula económica que se aplica, por ejemplo, por mi experiencia, si en una licitación el precio son 50 puntos, y se usa una fórmula económica de Regla de tres Proporcional, sé de antemano que un 2% de diferencia en el precio es exactamente 1 punto en la económica, con lo que, en un rango normal, va a haber poca diferencia entre las empresas. Sin embargo, si se usa la fórmula de diferencia con licitación, ese mismo 2% se puede convertir en 15 puntos. Por lo tanto, es muy importante saberlo de antemano.

Actualmente, en I-SEC , estás especializado en el sector del transporte, en el que destaca el transporte aéreo. Si no estoy mal informado lleváis la seguridad del 30% de los aeropuertos españoles. Siendo éste último un sector tan regulado ¿cómo afecta este factor a la realización de las licitaciones?

Si en algo se destacan los servicios que hay que realizar en AENA, es la necesidad de la excelencia en la prestación de los mismos. Por ello, creo que hay pocas empresas que operan en este sector, como bien dices, es un sector muy regulado, y no sólo por el cliente o seguridad privada, también tienes a otros organismo como AESA que constantemente están auditando la seguridad en los aeropuertos de manera muy exigente, tal y como debe de ser en sector tan crítico como este, ya que la seguridad aeroportuaria tiene un impacto mundial, un fallo de seguridad en un aeropuerto de España puede repercutir en cualquier lugar del mundo.

En sí, las realización de las licitaciones, hasta la última que se hizo en 2023 ha sido como casi todas, pero en 2023 pusieron en marcha un nuevo tipo de licitación denominado Dialogo competitivo, con una oferta inicial, una segunda fase en la que las diferentes licitadoras podían proponer cambios a los pliegos, que provocaron una segunda licitación con los pliegos optimizados por las empresas. Ha sido un procedimiento novedoso e interesante, en el que hemos aprendido otra forma de licitar distinta.

En los dos últimos años has estado compaginando tu labor de realización de licitaciones con la de controller, desarrollando un sistema propio de ayuda al control de los servicios – está claro que no dejas de investigar- partiendo de la ERP* de la Compañía. ¿Puedes indicarnos en qué te facilita este sistema tu trabajo?

Sobre todo, en conocer todas los aspectos que afectan a los costes en cada contrato y zona que tenemos. Por ejemplo, en vigilancia, un gran factor de coste es el absentismo, saber exactamente el coste del absentismo es fundamental para hacer un buen escandallo económico en una oferta, y por ejemplo, nada tiene que ver el coste que tenemos en Madrid o en Barcelona, y eso es importante tenerlo en cuenta a la hora de hacer los estudios económicos de los proyectos.

Espero que además de trabajar, conseguirás sacar tiempo libre para tus aficiones. Háblanos de ellas.
Pues en primer lugar mi familia, especialmente tengo una hija de 3 años, e intento disfrutar todo lo que pueda con ella.

Como gran afición destacaría la montaña, me encantar correr por el monte y hacer carreras. Aquí en el norte, soy un privilegiado en este sentido, y aunque he estado un par de años más tranquilo, ahora estoy retomando esta afición, y ya tengo previstas un par de ultras de montaña, especialmente una en Picos de Europa, donde nunca he corrido.

En el actual mundo del WhatsApp y las redes sociales ¿Qué opinas de la actividad en ellas de la Asociación?
Tengo que reconocer que no soy muy aficionado, más bien lo contrario, a las redes sociales. Lo único que puedo decir del grupo de Whatsapp de la asociación, es que creo que es muy buena iniciativa, y sobre todo para ayudarnos entre los asociados.

También es verdad, que como mi labor, hoy en día, está más bien desconectada de la labor de ingeniero de seguridad, pues soy poco activo en este campo.

Finalmente, y como petición obligada en estas entrevistas ¿tienes alguna propuesta sobre las actividades de la asociación que nos ayuden a mejorar?
En este sentido, creo que las actividades de formación, que se han empezado a poner en marcha son muy interesantes, como son las de análisis de riesgos previos. En este sentido, este tipo de actividades que ayuden a mejorar en nuestro trabajo siempre son buenas.

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

Estrategia Nacional de Protección Civil

El Departamento de Seguridad Nacional publicó el pasado mes de octubre el documento Estrategia Nacional de Protección Civil 2024. Elaborada por la Dirección General de Protección Civil y Emergencias, con la colaboración de los Ministerio y Organismos implicados en la materia.

"La Estrategia Nacional de Protección Civil desarrolla las actuaciones que debe realizar la Administración General del Estado en este ámbito de la seguridad pública y analiza las principales amenazas y riesgos de origen natural, humano y tecnológico que pueden dar lugar a emergencias y catástrofes en nuestro país, así como las líneas de acción estratégicas para integrar, priorizar y coordinar todos los esfuerzos para optimizar los recursos disponibles en esta Administración para su gestión".

+información

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR
Y OTROS ASUNTOS DE INTERÉS

Tecnologías Biométricas Seguras
para el Control de Acceso

El Centro Criptológico Nacional ha publicado el pasado diciembre el documento "Tecnologías Biométricas Seguras para el Control de Acceso"

Entre los diferentes aspectos que trata, cabe destacar los relativos a las plantillas biométricas (RBR) y su cumplimiento, en determinadas condiciones, de la legislación de protección de datos personales y el Reglamento Europeo de Inteligencia Artificial.

Así, en su Punto 4, página 8, puede leerse *"Los sistemas de control de acceso basados en la obtención de una plantilla biométrica RBR a partir de una determinada característica biométrica de la persona, cumplen con los exigido en materia de protección de datos por el Reglamento General de Protección de Datos5 y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales6, gracias a las siguientes características:..."* Respecto a l reglamento Europeo de IA, el punto 5 recoge que *"los sistemas de identificación biométrica no remotos en los que existe participación activa del usuario, así como los sistemas de verificación biométrica no están prohibidos y están calificados de riesgo bajo o nulo".*

+información

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Y OTROS ASUNTOS DE INTERÉS

La gestión de la ciberseguridad de los sistemas de seguridad física

Recomendaciones y casos de uso

Publicado por el Departamento de Seguridad Nacional el documento "La gestión de la ciberseguridad de los sistemas de seguridad física. Recomendaciones y casos de uso"

El documento elaborado por el **Foro Nacional de Ciberseguridad**, responde a la línea de acción 7 de la **Estrategia Nacional de Ciberseguridad: desarrollar una cultura de ciberseguridad.**

Es de destacar que este documento responde al interés de la Administración Pública, a través del **Departamento de Seguridad Nacional (DSN)** y al **Centro Criptológico Nacional (CCN)**, dependiente del **Centro Nacional de Inteligencia (CNI)**, ante el problema de los ciberataques a los Sistemas de Seguridad Física tanto para comprometer a las instalaciones y activos que protegen, como para ser vehículo de entrada a otros activos informáticos de las empresas.

En el estudio que ha llevado la redacción de este importante conjunto de recomendaciones, quizá algún día base para cambios legislativos, ha sido de gran importancia el impulso de la **Fundación Borredá** como coordinador del trabajo junto al **DSN**, y la sensibilización promocionada por **AEINSE** a partir de la **Guía G10/21 de Buenas Prácticas de Ciberseguridad en Proyectos de Sistemas de Seguridad Física** elaborada en 2021, así como su presentación en el **SICUR** de 2022.

Entre los autores y colaboradores del documento elaborado por el Foro Nacional de Ciberseguridad se encuentran nuestros socios **Raúl Aguilera, Alfonso Bilbao, Enrique Bilbao** y **Benjamín Suárez.**

+información

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

Sedexpro 25

Del 26 al 28 de marzo tendrá lugar la Feria Internacional de Seguridad, Defensa y Emergencias. Como en ocasiones anteriores abrirá sus puertas en el recinto Feria Internacional de Galicia – ABANCA- ubicado en Silleda (Pontevedra).

Además de la activad expositiva de material y equipamiento de seguridad pública y privada, seguridad laboral, protección civil, emergencias, detección y protección de incendios, etc. tendrán lugar talleres y conferencias que serán de gran interés, así como exhibiciones y simulacros.

Más información y registro de visitantes

AEINSE
Asociación Española de Ingenieros de Seguridad

AGENDA DEL SECTOR

El Foro Económico Mundial ha publicado la nueva edición de su Informe de Riesgos Globales (The Global Risks Report 2025).

Global Risk Report 2025

El Foro Económico Mundial ha publicado la nueva edición de su Informe de Riesgos Globales (The Global Risks Report 2025).

El informe analiza los principales riesgos a nivel mundial, en tres marcos temporales: inmediato (2025), a corto plazo (hasta 2027) y a largo plazo (2035), y presenta las conclusiones de la Encuesta de Percepción de Riesgos Mundiales 2024-2025, que recoge las opiniones de expertos de todo el mundo.

+información

LEÍDO, VISTO Y OÍDO EN...

SEGURIDAD

LA SEGURIDAD FÍSICA "SECURITY" EN UN EDIFICIO

INGENIERO IVAN BALLESTEROS

Durante el diseño, construcción o explotación de un edificio, suelen surgir dudas sobre el nivel de seguridad requerido, las instalaciones necesarias, así como el papel que juegan los elementos constructivos. En este sentido, es recomendable que la seguridad se apoye en sus cuatro funciones:

1. Disuadir o convencer al adversario a que desista en el intento de ataque.
2. Detectar al adversario que ha decidido atacar el edificio.
3. Retardar al adversario a que continue el avance.
4. Responder con la finalidad de interrumpir el ataque.

La disuasión es un elemento que se consigue aplicando el enfoque CPTED "Crime Prevention Through Environmental Design" desde el diseño arquitectónico.

Las restricciones en el diseño, o la amenaza de un adversario decidido, requiere implementar la segunda función del sistema de seguridad, detectar al adversario.

La detección del adversario requiere de medidas de seguridad electrónica adecuadas a cada posición y a las tácticas esperadas en el ataque, así como la capacidad de transmitir los avisos de alarma para su evaluación y clasificación como Alarma Confirmada o como Falsa Alarma.

El retardo es el tiempo que se requiere en superar el elemento constructivo, con las capacidades y recursos que se esperan del adversario.

La respuesta tiene la finalidad de interrumpir el ataque

74 CUADERNOS DE SEGURIDAD

CUADERNOS DE SEGURIDAD

En la página 74 del número 379 encontramos un artículo de nuestro vicepresidente, **Iván Ballesteros** con el título **"LA SEGURIDAD FÍSICA - SECURITY – EN UN EDIFICIO"**, en el que aborda la importancia de incluir a un consultor de seguridad en el equipo de diseño, construcción o explotación de un edificio.

LEÍDO, VISTO Y OÍDO EN...

INSTITUTO NACIONAL DE CIBERSEGURIDAD

INCIBE presenta un estudio pionero

sobre la ciberseguridad de los juguetes conectados

En el presente estudio, **INCIBE** ha analizado 26 juguetes inteligentes con capacidad de manejar datos del usuario, grabar vídeo o audio, conexión Bluetooth o Wi-Fi o aplicación móvil para el manejo del dispositivo; evaluando sus puntos fuertes y aspectos de mejora y emitiendo recomendaciones para fabricantes y consumidores.

+información

LEÍDO, VISTO Y OÍDO EN...

IEEE Spectrum
FOR THE TECHNOLOGY INSIDER

Criptografia pos

El **Instituto Nacional de Estándares y Tecnología de Estados Unidos** (**NIST,** por sus siglas en inglés) anunció hoy la estandarización de tres esquemas de cifrado de criptografía poscuántica.

"Hoy en día, casi todos los datos en Internet, incluidas las transacciones bancarias, los registros médicos y los chats seguros, están protegidos con un esquema de cifrado llamado RSA (llamado así por sus creadores Rivest, Shamir y Adleman). Este esquema se basa en un hecho simple: es prácticamente imposible calcular los factores primos de un gran número en una cantidad razonable de tiempo, incluso en la supercomputadora más poderosa del mundo. Desafortunadamente, las grandes computadoras cuánticas, si se construyen, encontrarían esta tarea muy fácil, socavando así la seguridad de todo Internet."

Leer el artículo completo: **aquí**

Acceder a la página de NIST: **aquí**