AES ASOCIACIÓN ESPAÑOLA EMPRESAS DE SEGURIDAD

Número 86
Julio 2023

Boletín Informativo

Dinamizando la Industria de la Seguridad

Carta del Presidente

Estimados asociados,

Encaramos ya la segunda mitad de este 2023, muchos de vacaciones cuando leáis estas letras y otros esperando las suyas, que ya no tardarán. Os informo de cómo ha ido la primera mitad del año y las actividades acometidas por la Asociación:

1- Áreas de Trabajo:

- **Seguridad Electrónica:** fundamentalmente se han llevado a cabo varias reuniones con la Asociación Española de Ingenieros de Seguridad, AEINSE, conforme a las cuales se ha elaborado una línea de actuación conjunta, que tenéis detallada en la nota de prensa publicada en este Boletín, y que comenzará en septiembre con la sesión técnica organizada por las dos asociaciones sobre la Guía de Instalación de grados 3 y 4 publicada por AES hace unos meses.
- **Ciberseguridad:** enviado a los miembros del área de trabajo el ejemplo de Declaración de Aplicabilidad Categoría Baja ENS, publicado por el CCN - CERT. Próximamente se publicará la guía en la que ha estado trabajando esta área.
- **Seguridad Física:** la más activa, conjuntamente con otras dos asociaciones, FORO EFITEC y CEUSS, está redactando un protocolo de actuación para el cambio de los precintos en los contenedores de almacenamiento seguro para establecimientos obligados. Ya está muy avanzado y con

> *Estamos trabajando ya en la preparación del XIX encuentro Seguridad Pública – Seguridad Privada que tendrá lugar el 19 de octubre*

Boletín Informativo de AES
Revista Trimestral - Julio 2023 - núm. 86

Edita:
Asociación Española de Empresas de Seguridad
C/Alcalá, 99 2ºA - 28009 Madrid
Telf. 915 765 225
www.aesseguridad.es - aes@aesseguridad.es

Consejo de Redacción:
Antonio Escamilla Recio
Ignacio Jiménez castillo
Julio Pérez Carreño
Antonio Pérez Turró
Manuel Rodríguez-Reguero
Javier Ruiz Gil
Manuel Sánchez Gómez-Merelo
Iñigo Ugalde Blanco

Coordina:
Paloma Velasco Merino

Diseño, Maquetación y Realización:
ABADIA, Sistemas de Información
www.abadia-si.com

las mejoras que ha sugerido la UCSP se publicará en breve. Además, se ha trabajado en las modificaciones sugeridas por parte de los fabricantes de cajas y de puertas de seguridad para la revisión de la norma UNE EN50518.

- **CRAs:** se ha revisado la guía de prevención de falsas alarmas que se va a publicar, con la colaboración de las Fuerzas y Cuerpos de Seguridad, ACAES y UAS coincidiendo con las recomendaciones que se lanzan en la campaña de verano.

- **Normativa y certificación:** El grupo de trabajo de estudio de la norma UNE EN 50518 ha hecho ya cuatro reuniones que se están plasmando en un Excel en el que se recogen las modificaciones que vamos a sugerir desde AES.

2- En este mes de abril se publicará el tercer Boletín Informativo de AES del año, el número 86. Estáis todos invitados a participar con vuestros artículos técnicos en él.

3- Continúa creciendo nuestra presencia en Redes Sociales:

   a- Cuenta de Twitter: @aes_seguridad: 2.123 seguidores.

   b- Cuenta de LinkedIn: ASOCIACIÓN ESPAÑOLA DE EMPRESAS DE SEGURIDAD: 1.141 seguidores.

   c- Cuenta de Instagram: aesseguridad2021: 299 seguidores.

En cuanto a AES Fundación, seguimos con los trámites para su creación. El último ha sido la presentación de toda la documentación requerida en el registro del Ministerio de Justicia.

Estamos trabajando ya en la preparación del XIX encuentro Seguridad Pública – Seguridad Privada que tendrá lugar el 19 de octubre.

Ya sabéis que podéis hacernos llegar vuestras consultas y sugerencias por correo electrónico. Nos tenéis como siempre a vuestra entera disposición. Seguiremos trabajando en conjunto para continuar siendo el referente de la Industria de la Seguridad en nuestro país.

Un cordial saludo,

Iñigo Ugalde Blanco – Presidente de AES

en los medios

España es el sexto país europeo con más cámaras públicas de videovigilancia
Publicado en publico.es

Videovigilancia con Inteligencia Artificial para controlar aforos en Sonorama
Publicado en burgosconecta.es

Jumilla implantaráun sistema de videovigilancia de tráfico en lugares estratégicos
Publicado en sietediasjumilla.es

La policía de Vilanova inició un plan de videovigilancia de dos semanas para identificar a los conductores temerarios de Baión
Publicado en diariodearousa.com

Refuerzan la videovigilancia en la zona sur de Jerez para evitar más carreras de motos
Publicado en diariodejerez.es

Videovigilancia e intimidad personal: cómo evitar el enfrentamiento entre vecinos
Publicado en idealista.com

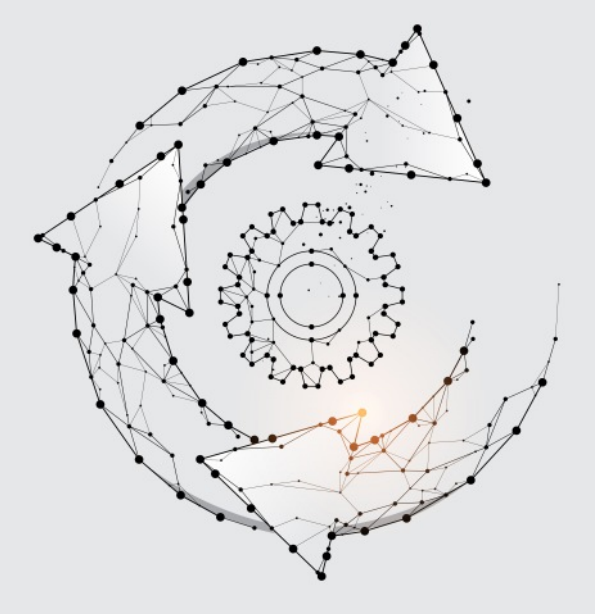
El TSJ de Cantabria admite la videovigilancia en los SUAP pero no la presencia física de vigilantes
Publicado en diariomedico.com

Videovigilancia para frenar el vandalismo en el parque de María Luisa y los Jardines de Murillo de Sevilla
Publicado en eldiario.es

Renfe digitaliza los sistemas de protección contra incendios de 400 estaciones
Publicado en renfe.com

Aprobada la modernización de los sistemas de seguridad del Hospital Universitario de Navarra
Publicado en diariodenavarra.es

AES (Asociación Española de empresas de Seguridad) y **AEINSE** (Asociación Española de Ingenieros de Seguridad) firmaron un convenio de colaboración como resultas del cual están trabajando en un acuerdo que incluye un plan de actuación conjunto, por el cual se comenzará activamente a colaborar en dos aspectos fundamentales: la retención y captación de talento de los ingenieros de seguridad por parte de nuestras empresas, focalizando en la formación y los departamentos de Recursos Humanos, y la realización de jornadas técnicas dirigidas a los ingenieros de seguridad, en las que las dos asociaciones aporten su experiencia.



En los primeros pasos de esta colaboración se abordará de forma conjunta la participación en común de los ingenieros de AES y de AEINSE en los cursos de formación continua (Sesiones Técnicas de corta duración muy especializadas), la difusión de la profesión de ingeniero de Seguridad en Universidades y Colegios Profesionales y, en general, la puesta en común de las acciones divulgativas de la tecnología de Seguridad.

AES y AEINSE tienen un conjunto de intereses comunes que hace muy interesante la colaboración de las dos asociaciones.

Estos intereses comunes hacen que ambas se hayan puesto el objetivo de abordar varios desafíos que les afectan, con el objetivo de ampliar las oportunidades en nuestra industria, entre otras:

- Carencia generalizada de Ingenieros de Seguridad.
- Necesidad de formación continua técnica, dada la velocidad del cambio tecnológico.
- Necesidad de profesionalización del sector y deseo de ambos colectivos de significarse ante competencias desleales.

Para todas aquellas personas que deseen informarse de las condiciones de ingreso en AEINSE, pueden visitar el siguiente enlace:

https://www.aeinse.es/solicitudes/quiero-ser-socio

NOTA DE PRENSA

Norma UNE-ISO 37002: el estándar mundial que ayuda a las organizaciones a conocer las conductas irregulares internas

La nueva Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, establece la obligatoriedad de implantar un "sistema interno de información" para conocer conductas irregulares en determinado tipo de organizaciones. La Norma UNE-ISO 37002 indica cómo se puede implantar un sistema de esas características.

El sistema de gestión que establece la norma es aplicable a todo tipo de organizaciones, independientemente del tipo, tamaño, naturaleza de su actividad y del sector al que pertenezcan (público, privado, sin ánimo de lucro).

Madrid, 10 de julio de 2023 – Tras la publicación de la nueva Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, cobra especial relevancia la Norma UNE-ISO 37002 *Sistemas de gestión de la denuncia de irregularidades. Directrices*. Se trata de un estándar mundial compatible y complementario con la legislación, que ofrece directrices sobre cómo establecer, mantener y mejorar un sistema de gestión de la denuncia de irregularidades en las organizaciones, basado en los principios de confianza, imparcialidad y protección y referido a todas las fases necesarias para la gestión de las mismas: la recepción, la evaluación, el tratamiento y la conclusión.

El texto legal establece la obligatoriedad de implantar un "sistema interno de información" para conocer conductas irregulares en determinado tipo de organizaciones; en este marco, la Norma UNE-ISO 37002 indica cómo se puede implantar un sistema de esas características. Además, este sistema puede ser una herramienta de gobernanza y de gestión muy importante para otras muchas organizaciones que quedan fuera del ámbito de la ley.

La Ley 2/2023 incorpora al derecho español la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, que impulsa los procesos de información (alerta/denuncia) y ofrece protección al informante (alertador/denunciante), al entender que esos procesos son claves a la hora de impulsar investigaciones y asegurar una aplicación coherente del derecho europeo.

La Norma UNE-ISO ayuda a hacer efectiva esta idea que subyace en la nueva legislación de protección al denunciante, donde la colaboración es un elemento clave en el Estado de derecho porque puede ayudar a erradicar conductas irregulares dentro de las organizaciones que perjudican el interés general. A veces sucede que determinados comportamientos que se producen en el seno de las organizaciones y que constituyen irregularidades (vulneraciones de la legislación, incumplimientos de códigos de conducta o acciones u omisiones que ocasionan daño, entre otros) permanecen ocultos y no llegan a conocerse internamente. En muchas ocasiones, la falta de confianza o el miedo a las represalias impide que los empleados de una organización u otras personas conocedoras de esas irregularidades, las pongan de manifiesto.

Este estándar mundial ofrece respaldo a todos los pasos del proceso de denuncia, exige la existencia de una función de gestión de denuncias independiente y dotada de recursos, y exige, asimismo, un seguimiento, medición, análisis y evaluación de resultados para lograr su mejora. También incluye un enfoque a riesgos, que cobra especial relieve en la identificación de los riesgos de perjuicio a los que pueden enfrentarse los denunciantes.

Además, aconseja que se establezcan las medidas adecuadas de sensibilización y formación de todas las personas que realizan trabajos bajo el control de la organización, para que comprendan cuáles son los objetivos del sistema, cuál es la importancia de contribuir al mismo y qué implicaciones tiene incumplir los requisitos. Si los órganos de gobierno no ofrecen confianza, imparcialidad y protección, y si el personal no conoce o no confía en el sistema de denuncias, no habrá denuncias y, tanto, no existirá un sistema eficaz de información.

Las recomendaciones que establece son aplicables a todas las organizaciones independientemente del tipo, tamaño, naturaleza de la actividad, y de si son públicas, privadas o sin fines de lucro. Por tanto, pueden aplicarla todas aquellas entidades que tienen que cumplir con la nueva legislación y, también, aquellas otras que, aunque no están obligadas a aplicarla, desean demostrar prácticas de gobernanza sólidas y éticas ante la sociedad, los mercados, los reguladores, los propietarios y otras partes interesadas.

La Norma UNE-ISO 37002 puede ser de especial interés para aquellas organizaciones que tengan implantado un sistema de gestión de *compliance*. Su aplicación puede incrementar la eficacia de los sistemas de gestión de *compliance* definidos en otras normas y que incorporan la denuncia de irregularidades como un elemento de información clave (UNE-ISO 37301 Sistemas de gestión del *compliance*. Requisitos con orientación para su uso; UNE 19601 Sistemas de gestión de *compliance* penal. Requisitos con orientación para su uso; UNE-ISO 37001 Sistemas de gestión antisoborno. Requisitos con orientación para su uso; UNE 19602 Sistemas de gestión de *compliance* tributario. Requisitos con orientación para su uso; PNE 19603 Sistemas de gestión de *compliance* en materia de libre competencia. Requisitos con orientación para su uso; o PNE 19604 Sistemas de gestión de *compliance* socio laboral. Requisitos con orientación para su uso).

Sobre la Asociación Española de Normalización, UNE

La Asociación Española de Normalización, UNE, es una organización global cuyo propósito es desarrollar normas técnicas o estándares que contribuyan al progreso compartido de la sociedad y a la creación de un mundo más seguro, sostenible y competitivo.

Las normas recogen el consenso del mercado sobre las mejores prácticas en aspectos clave para la competitividad de las organizaciones y para los intereses de toda la sociedad, siendo el resultado del diálogo y la colaboración conjunta de los sectores económicos y las Administraciones públicas.

Con la participación de más de 13.000 profesionales en sus mesas de trabajo, UNE es el representante español en los organismos de normalización internacionales (ISO e IEC), europeos (CEN-CENELEC y ETSI) y americanos (COPANT).

Para más información:

Asociación Española de Normalización, UNE
Vanesa Guerrero
Directora de Comunicación
Tel. 699 99 58 72
comunicacion@une.org
www.une.org

PROA Comunicación
Julia Montoro
Tel. 686 85 45 54
julia.montoro@proacomunicacion.es

Seguridad Global. Decálogo de asignaturas pendientes

Cada año que finalizamos un curso o ciclo académico parece obligado hacer resumen de aquellas asignaturas que tenemos pendientes, bien por falta de estudio, recursos o tiempos, o por simple procrastinación.

Los grandes problemas mundiales pasan en la actualidad por el establecimiento de un nuevo orden y una nueva perspectiva que derive en una nueva seguridad integral, integrada y globalizada.

El hecho es que, si hacemos un breve análisis, veremos que al menos una decena de esas asignaturas pendientes sigue casi igual que hace tiempo, lo que nos lleva a pensar que no les hemos dado la prioridad que les corresponde para poder hacer un buen balance.

Manuel Sánchez Gómez-Merelo
Consultor Internacional de Seguridad

Este es el caso de la Seguridad con mayúscula, ese amplio y universal concepto y objetivo que arrastramos y arrastraremos en todo tipo de actividad de nuestra sociedad.

Veamos con un poco de detalle la realidad de nuestro decálogo de asignaturas pendientes en materia de seguridad:

Riesgos y amenazas globales

Primero fue la 'pandemia' de COVID-19; luego, cuando comenzaba la recuperación, irrumpió el conflicto en Ucrania y las sanciones económicas a Rusia, para finalmente ingresar en un período de elevada inflación que arrojará a la economía mundial a un escenario de recesión por el alza de la tasa de interés internacional.

Estos impactos negativos han provocado una profunda alteración en la seguridad humana y ciudadana.

Con los recientes incrementos de amenazas y su complejidad, la falta de integración y unificación deja de ser un simple inconveniente para convertirse en un grave problema, al aumentar los riesgos y destacar vulnerabilidades para impedir respuestas coordinadas e integrales ante las contingencias derivadas de la materialización de los riesgos y amenazas.

El desafío de estas amenazas complejas tiene como mejor respuesta el planteamiento de una seguridad global y, en sus objetivos, su mejor valor añadido.

En este sentido, siendo imprescindible conocer los riesgos a los que están sometidos los sistemas de funcionamiento de las organizaciones para poder gestionarlos, están apareciendo multitud de guías formales e informales, aproximaciones metodológicas y herramientas o plataformas de soporte, para tratar de objetivar el análisis y la evaluación, especialmente en tiempo real.

Cultura de seguridad y concienciación ciudadana

El objetivo es plantear la cultura de la seguridad como un bien público, propiciando la evolución y desarrollo de un paradigma de seguridad compartido, que abarque de lo global a lo local. Los principales organismos centrados en el análisis del concepto de seguridad han dejado patente su carácter evolutivo y la necesidad de adaptarlo a las transformaciones acaecidas con la creciente globalización de la inseguridad.

Para ello, se impone la revisión de las políticas de seguridad, creando una novedosa cultura de seguridad integral e integrada, estableciendo los mecanismos de control y gestión de la seguridad física y lógica, y cuidando los sistemas, sin olvidar dimensionar la resiliencia.

Por Acuerdo del Consejo de Ministros, en mayo de 2021, se aprobó en España el Plan Integral de Cultura de Seguridad Nacional (Orden PCM/575/2021, de 8 de junio), a fin de servir de catalizador para la implantación progresiva de una cultura de seguridad inclusiva, participativa y colaborativa, todo ello con el fin de reforzar el Sistema de Seguridad Nacional, mejorar la coordinación y eficacia de la acción del Estado y la participación de la sociedad.

Para el desarrollo del Plan, se establece cuatro ámbitos de actuación: Formación, Comunicación pública y divulgación, Relevancia en el exterior y Participación, en los que se fomentará la colaboración y cooperación público-privada entre las comunidades de referencia.

Redefinición de la seguridad

De la convergencia a la seguridad global. Una necesaria redefinición y, sin duda, una nueva oportunidad para avanzar en la Seguridad Global de un mundo de retos colectivos y futuro incierto, con necesidad de entender las nuevas dinámicas sociales, económicas, energéticas y tecnológicas, para propiciar el desarrollo de ese amplio concepto de la nueva seguridad que va a estar presente de ahora en adelante.

También hemos de aprovechar la oportunidad para avanzar de la seguridad global a la seguridad local, enfocando una prevención + protección eficiente para los ciudadanos, dado que, en estos momentos, las amenazas se presentan con muchas dimensiones y formas, en ámbitos como la geopolítica, la delincuencia y terrorismo, las catástrofes naturales y, más recientemente, las pandemias mundiales. Hemos de pensar en global pero, actuar en local.

Nuevos retos y exigencias

Debemos ser conscientes de que en el mundo actual se están produciendo cambios profundos, no eventuales, y que es necesario contribuir de una forma más eficaz y realista a la mejora de la seguridad global. Desde esta perspectiva hemos de ayudar a instituciones y organizaciones a rediseñar nuevas estrategias en el nuevo mundo globalizado.

En este sentido, uno de los objetivos es dotar a las organizaciones de una metodología y tecnología sostenible de seguridad, haciendo converger a proyectistas, proveedores, integradores y gestores de soluciones con los propios usuarios que demandan adecuadas soluciones a sus nuevos retos y exigencias.

El pasado año, en la celebración de la XXX Cumbre de la OTAN en Madrid, se redefinió la seguridad mundial. Durante este encuentro de alto nivel se aprobó el nuevo Concepto Estratégico de la OTAN, un documento clave que define los desafíos de la organización internacional para la próxima década.

Una redefinición y, sin duda, una nueva oportunidad para avanzar en la Seguridad Global de un mundo de retos colectivos y futuro incierto con necesidad de entender las nuevas dinámicas sociales, económicas, energéticas y tecnológicas en el desarrollo de ese amplio concepto que es la seguridad global que va a definir el presente y futuro próximo y todas las asignaturas pendientes.

Todo ello, sin obviar la oportunidad para acometer los nuevos retos de un mundo que ha cambiado profundamente, en una Europa que tiene por delante la urgencia de terminar con la guerra en Ucrania, así como otras asignaturas pendientes igualmente importantes como la adopción nuevas estrategias y medidas a adoptar ante las permanentes oleadas de inmigrantes que buscan la supervivencia en un mundo mejor.

Adecuación de normativa y legislación

Otra asignatura pendiente de forma permanente es la necesaria actualización de la legislación en materia de seguridad en todos sus aspectos y frentes, así como la dinamización de nuevas normativas de aplicación, principalmente, para el control y gestión de las seguridades.

Como objetivo prioritario y asignatura pendiente se encuentran desde la Ley Orgánica 4/2015 de Seguridad Ciudadana, pasando por la Ley 5/2014 de Seguridad Privada y su falta de desarrollo reglamentario, hasta la posible adecuación a nuevo orden europeo de seguridad de la Ley 8/2011 de Protección de Infraestructuras Críticas, la Ley 7/2021 de Protección de Datos y el desarrollo de la legislación y normativa o Ley de Ciberseguridad de la UE.

Cabe destacar que los cambios que produjo esta directiva europea fueron tan importantes que la propia normativa sobre protección de datos española tuvo que actualizarse para adaptarse a ella. El gran desconocimiento de la normativa sobre protección de datos, así como la privacidad de los mismos, es aún una asignatura pendiente para muchas organizaciones.

En todos los casos, su inicial establecimiento supuso un notable avance para el desarrollo de la seguridad en España, y se reconoció la madurez de las organizaciones de seguridad, lo que ayudó a superar el concepto de control para pasar a una integración operativa y un planteamiento de servicios en asociación público-privada, siempre desde una perspectiva holística, especialmente en lo que se refiere a la protección de los activos de las organizaciones, para garantizar el funcionamiento de las infraestructuras críticas frente a todo tipo de riesgos.

Por otro lado, también la Ciberseguridad es la asignatura pendiente de la transformación digital, con gran preocupación por su dimensión y aplicación transversal para las organizaciones y ciudadanos.

Nuevas soluciones innovadoras

La industria de las seguridades se encuentra en una posición única para identificar los potenciadores más importantes, los eventos disruptivos y los desarrollos derivados de las nuevas tendencias, exigencias y retos, que darán forma al nuevo panorama de la seguridad global.

Especialmente, 2023 seguirá siendo un año en el que se irá consolidando la importancia de la seguridad para proteger los diferentes ámbitos institucionales, industriales y comerciales, con nuevas aplicaciones tecnológicas y sistemas de integración y monitorización global

Así, cabe destacar:

- La gestión de accesos securizados, que ya es y será una necesidad para las organizaciones y se espera que su adopción sea impulsada por medidas regulatorias internacionales.

- La Protección de las infraestructuras críticas con nuevas exigencias de protección y desarrollo de los planes de seguridad, contingencia y continuidad.

- La implementación de soluciones “zero trust” para facilitar la visibilidad y garantizar el mejor control y gestión de la seguridad global de forma integral e integrada en todo el proceso.

- La seguridad de acceso “just in time” a los recursos de IT justo en el momento en el que se necesitan.

- La autentificación de procesos, principalmente para la ciberseguridad de los dispositivos y aplicaciones conectados.

- La capacidad de establecer la autentificación de los sistemas de control de acceso biométrico y la videovigilancia, cada vez más fundamentales.

- La ciberseguridad estructural OT que requerirá de nuevas soluciones personalizadas por sectores de actividad.

- La combinación de IoT, la nube y las tecnologías móviles está impulsando de forma continua la transformación digital en la industria de la seguridad y, por tanto, presentando nuevos retos.

En cualquier caso, caminar hacia esta seguridad global, requiere de propuestas viables y prácticas y, sobre todo, de mucho compromiso por parte de los especialistas de las distintas seguridades o disciplinas en las organizaciones, teniendo siempre en cuenta los numerosos riesgos y las amenazas que, como nuevos retos, aguardan hoy en día a cualquier organización.

Nuevos líderes para la seguridad

Para la nueva visión y misión de la seguridad integral e integrada, junto a la inteligencia operativa y la gestión global, es preciso que los responsables de la seguridad corporativa cambien su habitual posición de una postura funcional, especializada y experta, a una posición con visión global de la organización, que observe y analice de manera transversal la información y, dentro de ella, lo que puede afectar de manera global y sostenible a la continuidad.

Es cada vez más amplio y complejo el asunto de determinar quién debe ser el encargado de controlar la seguridad de las organizaciones, y es ahora cuando debemos subrayar la importancia del nuevo perfil del Director Ejecutivo de Seguridad Global (CSO, CISO, CTI, etc.) que deberá poseer una formación, conocimientos, competencias y habilidades adecuadas para garantizar esa seguridad global y proactiva (prevención + protección) de todos los activos de la organización, generando las respuestas correctas ante los incidentes y contingencias críticas.

En este sentido, el nuevo «concepto de la seguridad global» ya está iniciando el cambio de rol que los profesionales y especialistas de seguridad deben desempeñar incrementando valor compartido a la organización.

En definitiva, estamos en los planteamientos hacia un Director de Seguridad Global, con visión holística, multidisciplinar y alta capacidad de gestión, reportando directamente a la Dirección General (CEO) y gestionando el riesgo global de la organización.

Digitalización e Inteligencia Artificial (IA)

La transformación digital ha traído consigo un cambio a implementaciones en la nube y nuevos modelos de servicio que ha brindado oportunidades para gestionar el control en aplicaciones de seguridad, activos físicos y datos, así como el uso de nuevos formatos ha permitido una autenticación confiable y ágil.

La implementación en los últimos años de la Inteligencia artificial (IA) en aplicaciones sociales y de seguridad se ha infiltrado en multitud de dispositivos y seguirá poniendo a disposición una auténtica invasión de esa inteligencia artificial a todos los niveles, incluido el de la seguridad.

La legislación y la reglamentación relacionadas con el desarrollo y el uso de tecnologías y aplicaciones basadas en la inteligencia artificial en materia de seguridad en el ámbito internacional y regional, es una asignatura pendiente.

Colaboración público-privada

La seguridad es y será el nuevo reto, principalmente en los ámbitos públicos, ciudadanos y empresariales. Sus responsables se hacen más importantes en todas las entidades, con la misión de prevenir los riesgos y amenazas y garantizar la gestión e intervención, minimizar los daños o pérdidas y garantizar la seguridad.

Es un hecho claro que, ante la gravedad de los nuevos riesgos y las amenazas que a diario se deben afrontar, es una obligación la colaboración a nivel operativo de la Seguridad Privada con la Seguridad Pública.

El presente y futuro de la seguridad ciudadana, ofrece una serie de ventajas muy positivas debido a la existencia de proveedores con una alta especialización, profesionales responsables de los sectores públicos y privados participantes e implicados en los proyectos en clara alianza de colaboración entre especialistas públicos y privados. Es a través de la colaboración operativa que se facilitarán las actuaciones necesarias para poder optimizar la respuesta ante los nuevos retos en la seguridad global y, especialmente, en la protección de infraestructuras críticas.

España es una potencia en seguridad pública y privada pero, precisa avanzar en sus asignaturas pendientes.

Formación especializada

Los nuevos retos y nuevas respuestas globales hacen precisa también una visión compartida, y la preparación adecuada de cada vez más profesionales ejecutivos y operativos, que han de acreditar una formación y capacitación especializada, no lineal, basada en estrategias y pensamientos exponenciales abiertos y flexibles que les convierta en los lideres de la seguridad que hoy precisamos.

Hay que adecuar nuevos programas de formación de seguridad global y promover la educación y concienciación de las personas en relación con los diferentes tipos de delitos, sus consecuencias y las medidas preventivas que pueden tomar para protegerse, a sí mismos, y a sus comunidades, creando una nueva cultura de seguridad.

destacados

BOE-A-2023-16643 Real Decreto 653/2023, de 18 de julio, por el que se modifica el Reglamento de Armas, aprobado por el Real Decreto 137/1993, de 29 de enero.

Publicado en boe.es

DEBATE SOBRE LA DIGITALIZACIÓN DE LAS CRAS

Publicado en issuu.com. Cuadernos de Seguridad

Directiva NIS 2: la identidad es la clave.

Manuel Rodríguez Reguero.
Miembro de la junta directiva y coordinador del Área de Ciberseguridad de la Asociación Española de empresas de Seguridad (AES).

Publicado en seguritecnia.es

“La excesiva regulación no es buena porque limita a la tecnología, pero es necesaria”

Íñigo Ugalde.
Presidente de la Asociación Española de empresas de Seguridad (AES)

Publicado en seguritecnia.es

MINISTERIO
DEL INTERIOR

DIRECCIÓN GENERAL
DE LA POLICÍA
COMISARÍA GENERAL DE
SEGURIDAD CIUDADANA
Unidad Central de
Seguridad Privada

Informe: Plazos de adecuación a grado de los sistemas de seguridad electrónica, en el ámbito de la seguridad privada.

Con la aproximación del plazo marcado por la Orden INT/826/2020, de 3 de septiembre, por la que se modifican, en lo relativo a plazos de adecuación de medidas de seguridad electrónica, la Orden INT/314/2011, de 1 de febrero, sobre empresas de seguridad privada, la Orden INT/316/2011, de 1 de febrero, sobre funcionamiento de los sistemas de alarma en el ámbito de la seguridad privada, y la Orden INT/317/2011, de 1 de febrero, sobre medidas de seguridad privada**, todo ello para la adecuación de los sistemas de seguridad electrónica, parece acertado realizar una valoración de diferentes aspectos que pudieran afectar a las empresas de seguridad, así como a los usuarios de sus servicios.**

1.- Aspectos que deben ser tenidos en cuenta:

Dicha Orden Ministerial modifica los plazos de adecuación señalados, en su momento, por las ya mencionadas Órdenes Ministeriales 314, 316 y 317 del año 2011, fijando como último día para poder llevar a cabo esas **actualizaciones de los sistemas de seguridad electrónica**, **el día 31 de diciembre de 2023.**

Siendo así que la Disposición transitoria primera de la Orden INT/316/2011, relativa a la "Adecuación de sistemas ya instalados", una vez operada esa modificación, quedo definida, en su párrafo primero, de la siguiente forma:

"*Los sistemas de seguridad instalados y conectados a centrales de alarmas o a centros de control, antes de la fecha de entrada en vigor de esta orden**, en establecimientos obligados y no obligados, tendrán de plazo para adecuarse a lo dispuesto en los artículos 2 y 3 de esta orden hasta el 31 de diciembre de 2023".***

Ello supone que el **día 1 de enero de 2024, cualquier sistema de seguridad electrónica** que se encuentre conectado a una CRA o a un centro de control, **debería cumplir con lo dispuesto por, entre otros preceptos, el artículo 2 de la Orden INT/316/2011, respecto a los grados de los sistemas de seguridad**, toda vez que establece lo siguiente:

"1. La Norma UNE-EN 50131-1 establece cuatro grados de seguridad en función del riesgo, quedando en esta Orden asignados, además, en virtud de la naturaleza y características del lugar en el que se va a efectuar la instalación y de la obligación, o no, de estar conectados a una central de alarmas o centro de control, del modo siguiente:

a) Grado 1, o de bajo riesgo, para sistemas de alarma dotados de señalización acústica, que no se vayan a conectar a una central de alarmas o a un centro de control.

*b**) Grado 2**, de riesgo bajo a medio, dedicado a viviendas y pequeños establecimientos, comercios e industrias en general, que pretendan conectarse a una central de alarmas o, en su caso, a un centro de control.*

*c) **Grado 3**, de riesgo medio/alto, destinado a **establecimientos obligados a disponer de medidas de seguridad,** así como otras instalaciones comerciales o industriales a las que por su actividad u otras circunstancias se les exija disponer de conexión a central de alarmas o, en su caso, a un centro de control.*

CORREO ELECTRÓNICO:
of.cgsc.ucsp@oficial.dgp.mir.es
ucsp.coordinacion@policia.es

C/ Rey Francisco, 21
28008 - Madrid
TEL.- 91.582.09.69 / 70

*d) **Grado 4**, considerado de alto riesgo, reservado a las **denominadas infraestructuras críticas, instalaciones militares, establecimientos que almacenen material explosivo reglamentado, y empresas de seguridad de depósito de efectivo, valores, metales preciosos, materias peligrosas o explosivos,** requeridas, o no, de conexión con central de alarmas o, en su caso, a centros de control.*

2. Los grados exigidos en esta Orden para los sistemas de seguridad quedaran sujetos a lo establecido en la Disposición transitoria segunda de esta Orden".

A su vez, se deberá disponer, para cada uno de los elementos de seguridad instalados, en base a esa adecuación**, del certificado de producto que, emitido por el correspondiente ente certificador, acredite disponer del grado de seguridad exigido**.

2.- Los sistemas de seguridad deberían ser adaptados, teniendo en cuenta lo siguiente.

1º.- **Sistemas de seguridad ordinarios** (domicilios, mercantiles, entidades comerciales, industriales, etc.) **conectados a una central receptora de alarmas o centro de control,** habrían de disponer:

- De elementos de seguridad electrónica **de Grado 2.**
- De un **nuevo certificado de instalación,** en su caso**,** que acredite el Grado 2 del sistema de seguridad.
- De un **nuevo certificado de conexión**, en el caso de estar conectado el sistema a una CRA, todo ello, al verse afectado el propio sistema por los cambios operados en el mismo.

2º.- **Sistemas de seguridad específicos de establecimientos obligados a disponer de medidas de seguridad electrónica** (se debe tener en cuenta que existen establecimientos que no están obligados a disponer de sistemas de seguridad electrónica) que, conectados de modo ordinario a una CRA, o de modo excepcional a un centro de control, habrían de cumplir con:

- Disponer, en su totalidad, de elementos de seguridad electrónica de **Grado 3**.
- Emitirse, en su caso, por la empresa de seguridad correspondiente, el **certificado de instalación** que acredite, precisamente, ser un sistema de Grado 3.
- A su vez, parece acertado recordar que los establecimientos que están obligados a disponer de una unidad de almacenamiento de seguridad, de las reguladas por la Norma UNE-EN 1143-1 (cajas fuertes o cámaras acorazadas), además de conectar su sistema de alarmas a una empresa de seguridad autorizada para la actividad de central de alarmas o, en su caso, a una central, también autorizada, de uso propio, dicha instalaciones, **habrían de contar, entre sus elementos, con un sistema de registro de imágenes, de forma que puedan ser utilizados como elemento de verificación** por la central de alarmas a la que estuvieran conectados.
- En caso de conexión a CRA, se debería dispone **de un nuevo certificado de conexión emitido por la CRA, que acredite la correcta conexión**, una vez llevadas a cabo las modificaciones relacionadas con la adecuación del sistema (ha de señalarse que, en el caso de tener conectados a la CRA un sistema no adecuado, **este hecho podría ser considerado como la conexión de un sistema de seguridad NO HOMOLOGADO**).

3º.- **Sistemas de seguridad electrónica de las empresas de seguridad**:

En cuanto a las medidas de seguridad electrónica de sus sedes o delegaciones, éstas deberían adaptarse a lo señalado por la modificación operada en el apartado 2 de la **Disposición Transitoria Única de la Orden INT/314/2011**, por la Orden INT/826/2020, en cuanto a que: "*Las medidas de seguridad electrónica y los sistemas de alarma **instalados en las empresas de seguridad antes de la fecha de entrada en vigor de esta orden** tendrán de **plazo para adecuarse** a lo dispuesto en la misma hasta **el 31 de diciembre de 2023***.», de modo que habrían de cumplir con lo siguiente:

- Los elementos de seguridad electrónica habrían de ser, en general de **Grado 3, salvo las empresas de depósito de efectivo, valores, metales preciosos, materias peligrosas o explosivos, cuyo Grado habrá de ser 4.**
- Todo debería estar acreditado, mediante **certificado de instalación**, emitido por una empresa de seguridad, respecto que el sistema de seguridad es de Grado exigido y se dispone de doble vía de comunicación con la CRA.
- De igual forma, se debería disponer de **un nuevo certificado de conexión**, que acredite el buen funcionamiento de la misma (conexión) con la CRA, una vez operada las correspondientes adecuaciones del sistema.
- Cabe recordar, a su vez, que habrán de disponer de **doble vía de comunicación con la CRA**.

4º.- **Sistemas de seguridad de infraestructuras especiales, tales como:**

- **Infraestructuras críticas.**
- **Instalaciones militares.**
- **Establecimientos que almacenen material explosivo reglamentado.**
- **Empresas de seguridad de depósito de efectivo, valores, metales preciosos, materias peligrosas o explosivos,**

Todas ellas deberían:

- Disponer de elementos de Grado 4 en su sistema de seguridad electrónico, al menos, en todos aquellos casos que se puedan disponer de los mismos, al existir la correspondiente comercialización en el mercado actual. Para lo que habría de tenerse en cuenta lo descrito por el segundo párrafo de la **Disposición transitoria primera de la Orden INT/316/2011,** relativa a la "Adecuación de sistemas ya instalados", que contempla lo siguiente:

  "Cuando un sistema de seguridad necesite utilizar componentes que, en el momento de su instalación, no estén disponibles en el mercado, según las normas recogidas en el apartado primero del artículo 3 de esta Orden, se permitirá su conexión, siempre que tales elementos no influyan negativamente en su funciona-miento operativo. La permanencia de tales elementos en el sistema estará condicionada a la posible aparición de la especificación técnica que lo regule y a su disponibilidad en el mercado. Transcurrido el período de carencia de diez años establecido en el párrafo anterior, se deberá disponer del pertinente certificado emitido por un Organismo de Control acreditado en base a la Norma EN 45011, responsable de la evaluación de la conformidad de los productos y exhibirse en caso de ser requerido".

- Disponer de un certificado de instalación emitido por una empresa de seguridad, que acredite esa situación.

- De igual forma, se debería disponer de un nuevo certificado de conexión, en su caso, que acredite el buen funcionamiento de la misma con la CRA, una vez operada las correspondientes adecuaciones del sistema.

3º.- Obligaciones de las empresas de seguridad, según la Ley 5/2014, de Seguridad Privada.

Las empresas de seguridad deben cumplir el principio rector definido por el artículo 8.1 de la mencionada Ley, que establece: "*1. **Los servicios y funciones de seguridad privada se prestarán con respeto a la Constitución**, a lo dispuesto en esta ley, especialmente en lo referente a los principios de actuación establecidos en el artículo 30**, y al resto del ordenamiento jurídico***".

Lo que conlleva que las **mismas han de cumplir con la exigencia de adecuar los sistemas de seguridad, que afectan o intervienen en la prestación de los servicios** de seguridad que desarrollan.

Así mismo, **dicho texto legal contempla como prohibiciones** que afectan a las empresas de seguridad, las descritas en su punto 1, apartados c) y d), que se corresponden con:

*"c) La prestación de servicios de seguridad privada **incumpliendo los requisitos o condiciones legales de prestación de los mismos**.*
*d) El empleo o utilización, en servicios de seguridad privada, de medios **o medidas de seguridad no homologadas cuando sea preceptivo,** o de medidas o medios personales, materiales o técnicos de forma tal que atenten contra el derecho al honor, a la intimidad personal o familiar o a la propia imagen o al secreto de las comunicaciones, o cuando incumplan las condiciones o requisitos establecidos en esta ley y en su normativa de desarrollo"*.

De tal forma que **las empresas de seguridad no podrían prestar servicios de seguridad, en los que suponga incumplir los requisitos y condiciones dispuestos por la normativa para su prestación,** como ocurriría en el caso de conectar sistemas de seguridad a una CRA, sin que los mismos se ajusten a los requisitos fijados por la normativa.

Por su parte, el texto legal de 2014, al regular los servicios de instalación y mantenimiento, establece en su artículo 46.1, lo siguiente:

*"1. Los servicios de instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas, centros de control o de videovigilancia, consistirán en la ejecución, por técnicos acreditados, de todas aquellas **operaciones de instalación y mantenimiento de dichos aparatos, equipos, dispositivos o sistemas, que resulten necesarias para su correcto funcionamiento y el buen cumplimiento de su finalidad**, previa elaboración, por ingenieros acreditados, del preceptivo proyecto de instalación, **cuyas características se determinarán reglamentariamente**".*

A este respecto**, cabe entender que las características técnicas determinadas reglamentariamente de los sistemas de seguridad, son las dispuestas, expresamente, por las Órdenes Ministeriales 314, 316 y 317**.

En cuanto a la homologación de sistemas de seguridad y su posible conexión a una central receptora de alarmas, el artículo 23 de la Orden INT/314/2011, contempla lo siguiente:

"***Cuando la instalación se conecte a central de alarmas, deberá ajustarse*** *a lo dispuesto en los artículos 40, 42 y 43 del Reglamento de Seguridad Privada,* ***considerándose homologados si reúnen las características determinadas en los artículos 22 y 24 de la presente Orden***".

De tal forma que **no parece pueda conectarse a una CRA, un sistema de seguridad que no cumple con lo establecido en dicho precepto**, donde se **exige el cumplimiento de la norma UNE EN 50131, que precisamente establece los grados de seguridad** que deben cumplir los sistemas de seguridad de usuarios, establecimientos obligados, etc.

4º.- Posibles infracciones:

a) Para las empresas de seguridad:

1º.- Cuando no adapten los sistemas de seguridad de sus sedes o delegaciones a lo exigido en la normativa, en tanto supone no adoptar medidas de seguridad de carácter obligatorio**.**

Artículo 57.1.j), de la LSP, que considera como infracción de carácter grave: "*La ausencia de las medidas de seguridad obligatorias, por parte de las empresas de seguridad privada y los despachos de detectives, en sus sedes, delegaciones y sucursales".*

2º.- Empresas de seguridad que realizarán la instalación de medios materiales no homologados, cuando la homologación es preceptiva, no instalando el grado de seguridad exigido.

Artículo 57.2.a) de la LSP, que considera como infracción de carácter grave: "***La instalación*** *o utilización de medios materiales o técnicos no homologados, cuando la homologación sea preceptiva",* en base al no cumplimiento de lo señalado por el articulo 23 de el artículo 23 de la Orden INT/314/2011, de empresas de seguridad.

3º.- Empresa de CRA que tiene conectados a su central sistemas de seguridad de usuarios que no disponen del grado de seguridad exigido, haciendo uso o utilización de esos medios en la prestación del servicio.

Artículo 57.2.a) de la LSP, que considera como infracción de carácter grave: "*La instalación o* ***utilización*** *de medios materiales o técnicos* ***no homologados****, cuando la homologación sea preceptiva*", toda vez que parece **que se utilicen**, en las actuaciones de recepción de las señales de alarmas, **elementos que no se encuentran debidamente homologados**, en virtud de lo dispuesto por el artículo 23 de la Orden INT/314/2011, de empresas de seguridad.

b) Usuarios de sistemas de seguridad:

1º.- Establecimientos obligados a disponer de medidas de seguridad:

Artículo 59.1.f) de la LSP, que considera como infracción de carácter muy grave: "***La falta de adopción o instalación de las medidas de seguridad que resulten obligatorias***". (pudiendo ser considera como falta de medidas de seguridad de carácter obligatorio, la disposición de aquéllas medidas o elementos que no se ajustan a lo señalado por la normativa).

2º.- Otras infracciones para usuarios de sistemas de seguridad.

Artículo 59.2.b) de la LSP, que considera infracción de carácter grave, la relativa a: "***La utilización de aparatos de alarma u otros dispositivos de seguridad no homologados"***. Toda vez que el usuario hace uso de ese tipo de elementos de seguridad, no homologado, atendiendo a la definición que realiza el artículo 2.13 de la LSP de "**elemento homologado**".

Artículo 59.3. a) de la LSP, que considera como infracción leve: "***La utilización de aparatos o dispositivos de seguridad sin ajustarse a las normas que los regulen****, o cuando su funcionamiento cause daños o molestias desproporcionados a terceros*".

5º.- Posibilidad de tramitar la baja de aquellos contratos de clientes (usuarios), que no acepten adecuar su sistema de seguridad al grado exigido por la normativa.

No parece desacertado que las empresas de seguridad (especialmente las que disponen de contratos de conexión de sistemas de seguridad a CRA o a centros de control o de videovigilancia), **para aquellos casos que los clientes no se adecúen al grado exigido por la normativa,** puedan gestionar la posible rescisión del contrato del servicio de seguridad, y como tal, comunicar la baja del mismo al Ministerio del Interior, al no adaptar sus sistemas a lo exigido por la normativa.

AGENDA 2023

FERIAS Y CONGRESOS

- II Congreso Internacional de Técnicas Avanzadas en Ciberseguridad, 6 y 7 de octubre de 2023: https://eicyc.com/ii-congreso-internacional-de-tecnicas-avanzadas-en-ciberseguridad/
- Smart City Expo World Congress y Tomorrow. Mobility World Congress, 7 a 9 de noviembre de 2023, Barcelona.
- Milipol Paris 2023, 14 al 17 de noviembre de 2023.
- SICUREZZA Fiera Milano, 15 al 17 de noviembre 2023.
- PMRExpo, la principal feria europea para la comunicaciones seguras, tendrá lugar del 28 al 30 de noviembre de 2023 en Colonia (Alemania).
- TECNOSEC DRONExpo 2024, 8 y 9 de mayo de 2024.

Hemos asistido

Pleno del Consell de Coordinación de Seguretat Privada de la Generalitat de Cataluña, 4 de julio

Desayuno de Nueva Economía Forum con José Vicente de los Mozos, Presidente del Comité Ejecutivo de IFEMA, 13 de julio

Presentación de las 10 medidas para la mejora institucional de la Fundación Hay Derecho, 14 de julio

en los medios

Twitter ahora es X: cuáles son los riesgos de ciberseguridad para los usuarios
Publicado en infobae.com

Ciberseguridad: ¿qué es una nube híbrida y cuáles son las ventajas de usarla?
Publicado en depor.com

Ciberseguridad: ¿qué es una nube híbrida y cuáles son las ventajas de usarla?
Publicado en 20minutos.es

Los hackers rusos que atacaron Interior también asaltaron las web del INE, Moncloa, la JEC y Correos
Publicado en elespanol.com

AES, Asociación Española de Empresas de Seguridad, es socio fundador de UAS (Unión de Asociaciones de Seguridad)

Agradecemos las colaboraciones que hacen posible esta edición trimestral y animamos a nuestros lectores a que nos remitan informaciones o artículos de opinión para su publicación en el boletín. AES no se hace responsable de las opiniones vertidas en este boletín.