NEWS ADSI FLASH
www.adsi.pro

Índice

Próximo "Martes con…" Templo Sagrada Familia - Xavier Edo – Aleix Riera

Seguridad Patrimonial de una joya del Modernismo, símbolo de Barcelona

Barcelona, martes 9 de febrero, a las 17:30 h.

Nuestros Patrocinadores

Próximo "Martes con…" Xavier Edo – Aleix Riera Junta Constructora del Templo de la Sagrada Familia

TEMPLO DE LA SAGRADA FAMILIA: Seguridad Patrimonial de una joya del Modernismo, símbolo de Barcelona

Barcelona, martes 9 de febrero, a las 17:30 h.
C/ Marina, acceso nº 1 (grupos)

Xavier Edo, Director de Seguridad y Responsable del Área de Seguridad, Licenciado en Criminología, Graduado en Investigación Privada, Master en Dirección Privada con 15 años de experiencia en Seguridad Pública y Privada.

Aleix Riera, Responsable del Área de Prevención de Riesgos Laborales, Arquitecto Técnico, Tecnico Superior en Riesgos Laborales, Post Grado en Coordinación de Seguridad y Salud, Safety Manager con 10 años de experiencia en Seguridad y Prevención de Riesgos.

Ambos se encuentran integrados dentro del departamento de Seguridad y Operaciones de la Junta Constructora del Templo de la Sagrada Familia.
Son las dos principales figuras dentro de la organización de la Junta Constructora que tienen como principal objetivo garantizar la Seguridad Integral dentro de la organización.

La coordinación entre ambas áreas, junto con el área de operaciones, garantiza la seguridad de las personas (visitantes y trabajadores), de los bienes (físicos y simbólicos) y de las diferentes instalaciones durante la actividad cultural, litúrgica y constructiva.

Cada uno de ellos utiliza diferentes medios para conseguir este objetivo.

Durante la visita nos explicarán como lo hacen.

Inscripciones cerradas

SICUR acoge una Jornada Internacional de Encuentros de Transferencia de Tecnología y búsqueda de socios

Salón Internacional de Seguridad
23-26 febrero 2016

HORARIOS
23, 24 Y 25 FEBRERO
10:00 A 19:00 H.
26 FEBRERO
10:00 A 15:00 H.

Organizada por la Fundación madri+d, se celebrará el 23 de febrero en el marco del gran referente internacional del sector de la seguridad.

SICUR reunirá, entre los días 23 al 26 de febrero, la más completa oferta de novedades y soluciones de vanguardia, en los pabellones de Feria de Madrid

La próxima edición de SICUR, Salón Internacional de Seguridad, que se celebrará del 23 al 26 de Febrero –martes a viernes- en Feria de Madrid, será el escenario de una Jornada Internacional de Transferencia de Tecnología, organizada por la Fundación para el Conocimiento madri+d, en el marco de las actividades vinculadas a su participación en la Enterprise Europe Network.

El objetivo de esta jornada es facilitar la comunicación y el encuentro entre empresas, centros de investigación y universidades del sector. La jornada, de carácter internacional, permitirá detectar potenciales oportunidades de colaboración y negocio mediante el desarrollo de entrevistas bilaterales presenciales previamente programadas.

Además, estos encuentros permitirán establecer contactos para el desarrollo de colaboraciones orientadas tanto a la prestación de servicios como a la puesta en marcha de proyectos de desarrollo tecnológico. Las empresas, universidades y organismos públicos de investigación, interesados en participar en esta jornada, deberán publicar al menos un perfil de oferta o demanda tecnológica antes del 17 de febrero. Dichos perfiles serán publicados en un catálogo online en continua actualización y, desde dicho catálogo, se podrán seleccionar perfiles tecnológicos de interés y solicitar reuniones.

Estas reuniones cortas, 30 minutos, permiten a las empresas y entidades un primer contacto para futuras cooperaciones. Esta iniciativa se apoya en el programa de trabajo de la Enterprise Europe Network, EEN, de la cual madri+d es un nodo activo. En 2014, en el marco de SICUR 2014, más de 80 entidades de 6 países participaron en los encuentros, celebrándose más de 120 reuniones. La EEN está formada por 600 organizaciones que ofrecen cobertura territorial en más de 50 países, acercando a las empresas servicios de asesoramiento, búsqueda de socios y apoyo a la transferencia de tecnología, como vía para incrementar su competitividad internacional.

Sobre SICUR
SICUR 2016, el gran referente internacional en España de la seguridad que organiza IFEMA en Feria de Madrid, volverá a reunir a empresas, asociaciones, profesionales y usuarios de seguridad en torno a un escenario de alta representación sectorial. La participación de 1.350 empresas de 19 países y un contenido especialmente marcado por la innovación y el avance tecnológico, ofrecen una perspectiva integral de las de las novedades de esta industria, en torno a las áreas de Seguridad Contra Incendios y Emergencias, Seguridad Laboral, Security, y Defensa. La oferta comercial se completa, con el programa de conferencias y debate que aborda Foro SICUR; la Galería de Nuevos Productos, que destaca una selección de propuestas de vanguardia en materia de protección y prevención, así como múltiples exhibiciones, presentaciones y demostraciones de gran dinamismo e interés profesional

Registro en el siguiente enlace

Instalación de un CCTV en montes de utilidad pública

Unidad Central de Seguridad Privada

ANTECEDENTES

Consulta efectuada por una Subdelegación del Gobierno, sobre la viabilidad para la instalación de un CCTV en montes de utilidad pública por parte de una Comunidad Autónoma, con objeto de garantizar la conservación y protección de los mismos, en virtud de las competencias que le otorga la Ley 43/2003, de 21 de noviembre, consistiendo dichos CCTV en un sistema de cámaras móviles, no idóneas para la captación de imágenes susceptibles de ser consideradas intromisiones ilegítimas en el derecho al honor, a la intimidad y a la propia imagen, y dotadas de un software inteligente capaz de discriminar vehículos determinados, enviando un mensaje de alerta cuando se detecte esa tipología de vehículo.

CONSIDERACIONES

Con carácter previo se participa que, los informes o respuestas que emite esta Unidad, tienen un carácter meramente informativo y orientativo –nunca vinculante- para quien los emite y para quien los solicita, sin que quepa atribuir a los mismos otros efectos o aplicaciones distintos del mero cumplimiento del deber de servicio a los ciudadanos.

En primer lugar, y desde el punto de vista de la normativa reguladora de seguridad privada, la Ley 5/2014 de 4 de abril, de Seguridad Privada, establece con relación a los servicios de seguridad consistentes en la videovigilancia, el artículo 42, indica lo siguiente:

"Artículo 42. Servicios de videovigilancia.
1. Los servicios de videovigilancia consisten en el ejercicio de la vigilancia a través de sistemas de cámaras o videocámaras, fijas o móviles, capaces de captar y grabar imágenes y sonidos, incluido cualquier medio técnico o sistema que permita los mismos tratamientos que éstas.

Cuando la finalidad de estos servicios sea prevenir infracciones y evitar daños a las personas o bienes objeto de protección o impedir accesos no autorizados, serán prestados necesariamente por vigilantes de seguridad o, en su caso, por guardas rurales.

***No tendrán la consideración de servicio de videovigilancia** la utilización de cámaras o videocámaras cuyo objeto principal sea la **comprobación del estado de instalaciones o bienes, el control de accesos a aparcamientos y garajes**, o las actividades que se desarrollan desde los centros de control y otros puntos, zonas o áreas de las autopistas de peaje. **Estas funciones podrán realizarse por personal distinto del de seguridad privada**.*

2. No se podrán utilizar cámaras o videocámaras con fines de seguridad privada para tomar imágenes y sonidos de vías y espacios públicos o de acceso público salvo en los supuestos y en los términos y condiciones previstos en su normativa específica, previa autorización administrativa por el órgano competente en cada caso. Su utilización en el interior de los domicilios requerirá el consentimiento del titular."

Añadiendo a continuación que:
5. La monitorización, grabación, tratamiento y registro de imágenes y sonidos por parte de los sistemas de videovigilancia estará sometida a lo previsto en la normativa en materia de protección de datos de carácter personal, y especialmente a los principios de proporcionalidad, idoneidad e intervención mínima.

6. En lo no previsto en la presente ley y en sus normas de desarrollo, se aplicará lo dispuesto en la normativa sobre videovigilancia por parte de las Fuerzas y Cuerpos de Seguridad."

De todo lo anterior, cabe determinar que la Ley de Seguridad Privada hace referencia a la utilización de cámaras de videovigilancia, para utilización en espacios privados, por lo que en el caso que nos ocupa, habrá de acudirse a normativa específica reguladora de la instalación de videocámaras en lugares públicos, prevista en la Ley Orgánica 4/1997, ya que versa sobre su uso concretamente en montes de utilidad pública.

De cualquier modo, y en este punto, resulta conveniente hacer mención de lo establecido en la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras, que en su artículo 4 señala que:

"Artículo 4. Principios de calidad, proporcionalidad y finalidad del tratamiento.

1. De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

2. Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

3. Las cámaras y videocámaras instaladas en ***espacios privados*** *no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida."*

Se refuerza aquí la postura en lo referido a la interdicción respecto de la obtención de imágenes de espacios públicos, si bien en este caso, desde el prisma de las instalaciones de CCTV ubicadas específicamente en espacios privados, teniendo en cuenta las salvedades que en el texto se enumeran.

Por lo tanto, y como consecuencia de lo anterior, con respecto a las videocámaras instaladas en espacios públicos, habrá de acudirse a la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos, que en su artículo 1, establece el objeto de la misma, indicando que:

"Artículo 1. Objeto.
1. La presente Ley regula la ***utilización*** *por las Fuerzas y Cuerpos de Seguridad de vídeo cámaras para grabar imágenes y sonidos en lugares públicos, abiertos o cerrados, y su posterior tratamiento, a fin de contribuir a asegurar la convivencia ciudadana, la erradicación de la violencia y la utilización pacífica de las vías y espacios públicos, así como de prevenir la comisión de delitos, faltas e infracciones relacionados con la seguridad pública.*

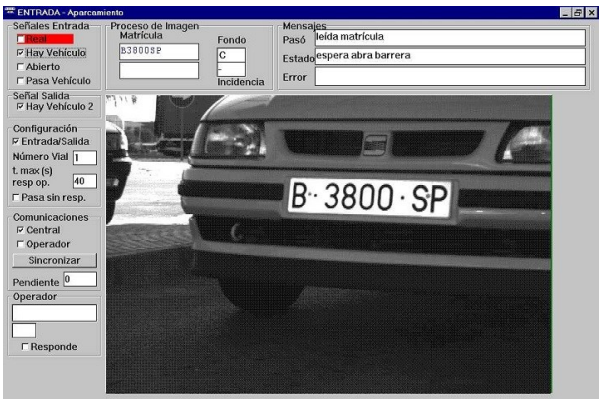
Asimismo, esta norma establece específicamente el régimen de garantías de los derechos fundamentales y libertades públicas de los ciudadanos que habrá de respetarse ineludiblemente en las sucesivas fases de autorización, grabación y uso de las imágenes y sonidos obtenidos conjuntamente por las videocámaras.

2. Las referencias contenidas en esta Ley a vídeo cámaras, cámaras fijas y cámaras móviles se entenderán hechas a cualquier medio técnico análogo y, en general, a cualquier sistema que permita las grabaciones previstas en esta Ley."

Dicha norma, hace referencia a la utilización de cámaras de videovigilancia, exclusivamente por parte de la Fuerzas y Cuerpos de Seguridad, con finalidad de contribuir a la seguridad ciudadana, con lo cual no parece existir identidad de objetivos con respecto al asunto consultado.

Del caso propuesto, se puede determinar que la captación por parte de las cámaras del CCTV, se trataría de imágenes que pueden ser consideradas como de vistas generales, panorámicas o paisajísticas de entorno forestal, sus vías y accesos de vehículos al mismo, con lo que no se podría distinguir actividades humanas singularizadas o individualizadas, por lo que en su uso no se pretenden obtener datos de carácter personal, de forma que puedan afectar a los derechos de imagen e intimidad de las personas.

A este respecto, incluso existen distintos ejemplos jurisprudenciales en los que los Tribunales, no han considerado que la comprobación de matrículas de vehículos suponga una vulneración de datos de carácter personal, sirviendo de ejemplo la sentencia núm. 5832, de 26 de diciembre de 2013, de la Audiencia Nacional, donde se indica que "*un número o placa de matrícula, si bien identifica un vehículo, en ningún caso identifica una persona, ya que el conductor del vehículo ni siquiera tiene porqué ser el titular del mismo, es decir, aquel a cuyo nombre figura dicho vehículo en la Dirección General de Tráfico.*"



En cuanto a su específica finalidad, refiere la consulta que dichas imágenes no vulneran los preceptos normativos en el ámbito de la protección de datos de carácter personal, siendo exclusivamente su pretensión, como se ha indicado, la de obtención de vistas generales del entorno, lo que no presenta, a priori, inconveniente alguno, dado que con frecuencia, este tipo de imágenes pueden ser obtenidas

actualmente, por la generalidad de las personas sin ninguna dificultad, al tener en muchos casos un carácter de difusión pública, mediante aplicaciones informáticas en la red INTERNET, en sitios webs tales como imágenes aéreas urbanas, estado de las pistas de esquí, paisajes rurales, aplicaciones tales como Google Maps o Google Earth o Street View.

Respecto a la instalación del CCTV, debe tenerse en cuanta que cualquier empresa que realice la instalación o el mantenimiento de cámaras de videovigilancia deberá inscribirse en el Registro de Instaladores de Telecomunicaciones, creado en la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, por lo tanto, si como es el caso, este sistema no fuera a ser conectado a centrales de alarma o centros de control o de videovigilancia, al ser otro el objeto de su finalidad, no es necesaria la inscripción de la empresa en el Registro de empresas de seguridad privada.

Debe indicarse además, que con respecto a la competencia para el conocimiento de los hechos relacionados con la grabación de imágenes, es materia que por imperativo legal corresponde al ámbito competencial de la Agencia Española de Protección de Datos, de conformidad con lo establecido en el artículo 37 de la Ley Orgánica 15/1999, de 15 diciembre, de Protección de Datos de Carácter Personal, por lo que cualquier asunto relacionado con el tratamiento de bases de datos de imágenes que supuestamente puedan estar grabando las vías y espacios públicos, deberá ser remitida a dicha institución.

CONCLUSIONES

A la vista de lo expuesto se pueden concluir los siguientes extremos:

1. Que en el caso expuesto en la consulta, se trata de una instalación de cámaras de titularidad pública, en espacios públicos, que no van a ser visionadas por las Fuerzas y Cuerpos de Seguridad, carentes de la finalidad de seguridad tanto privada como pública, ya que no pretenden la prevención de infracciones penales o de protección de la seguridad ciudadana.

2. Debido a que la finalidad última del sistema de CCTV que se pretende instalar, que en principio no va a producir vulneración alguna en los derechos de la intimidad personal y familiar de las personas, ya que lo que se pretende es la obtención de vistas generales y de control de accesos de vehículos, no parece existir inconveniente para su puesta en funcionamiento, desde el punto de vista de la normativa de seguridad privada.

3. Significar que, en cualquier caso, la competencia en materia de protección de datos de carácter personal, corresponde su control exclusivamente a la Agencia Española de Protección de Datos.

4. Que la finalidad de la normativa reguladora sobre la utilización de videocámaras en vías públicas no es la de prohibir la mera instalación, sino que por motivo de tal instalación su uso no pueda vulnerar los derechos fundamentales, en este caso de manera especial, los correspondientes a la intimidad personal y familiar y la propia imagen. En base a ello el legislador no ha considerado necesario prohibir situaciones en que el uso de las cámaras no vulnere tales derechos, o la incidencia sobre los mismos resulte insignificante.

5. Si los sistemas instalados fueran a ser visionados por las FF.CC.SS. con la finalidad prevista en la Ley Orgánica 4/1997 referida, se deberán seguir las preceptivas pautas establecidas en la misma para su autorización por la Subdelegación del Gobierno.

Este informe se emite en cumplimiento de lo dispuesto en el artículo 35.g) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, sobre derecho de información al ciudadano, y fija la posición y el criterio decisor de las Unidades Policiales de Seguridad Privada, en relación con el objeto de la consulta sometido a consideración. No pone fin a la vía administrativa ni constituye un acto de los descritos en el artículo 107 de la citada ley, por lo que, contra el mismo, no cabe recurso alguno.

Seguridad 2016: reducir vulnerabilidades y aumentar resiliencia

Manuel Sánchez Gomez-Melero
Consultor Internacional de Seguridad. Miembro experto de la Comisión Nacional de Seguridad Privada del Ministerio del Interior

Aunque el año 2015 será recordado como el año de las tragedias migratorias donde millones de refugiados están en movimiento y más de cinco mil personas han perdido la vida en su intento por obtener refugio o una mejor vida, quince años después del cambio de siglo, también constatamos que nuestras seguridades presentan mayores vulnerabilidades y nuestra resiliencia precisa aumentar.

La era de la Inseguridad

Si bien la globalización económica ha conducido a un aumento de la riqueza mundial sin precedentes, al tiempo está profundizando las desigualdades y la marginación, no sólo entre las personas, sino también entre países. En este sentido, el "circulo vicioso" de pobreza, desigualdad, frustración, criminalidad, exclusión, inseguridad y más pobreza en el que parecen estar inmersos muchos países está lejos de variarse.

No obstante, para hablar de la incidencia de la inseguridad por la globalización, antes debemos de definir el concepto "seguridad" como ámbito común de actividad de los diferentes actores y sectores. Así, hay que repensar los conceptos de bienestar, desarrollo, democracia y seguridad, desde el ángulo de la sostenibilidad, pues ha pasado a ser una tarea vital, aunque sigue siendo una asignatura pendiente.

También, en general, hay que tener en cuenta que, el término seguridad se asocia con otros conceptos como "seguridad pública", o "seguridad ciudadana", y también con otros más recientes como "seguridad sostenible" o "seguridad humana".

En cualquier caso, dentro de estos conceptos hay que tener en cuenta una clasificación general como es: Seguridad objetiva y seguridad subjetiva. La seguridad objetiva que es aquella que puede medirse cualitativa y cuantitativamente y es resultante de las acciones proactivas y reactivas programadas por el Estado y las Fuerzas de Seguridad Pública. Una seguridad objetiva que, según los datos y su forma de transmitirlos, puede llegar a causar alarma social. Por otra parte, la seguridad subjetiva es aquella que realmente es percibida por el ciudadano en su propia vivencia y estado de ánimo, y es más importante si cabe que la seguridad resultante de las cifras estadísticas y los estudios comparativos. Esta percepción de la inseguridad, es la interpretación por el sentido común de ciertas situaciones como inseguras, y es el resultado de un complejo proceso subjetivo de definiciones y atribuciones de valor, una puesta en valor personal y social de la realidad.

Por otro lado, la seguridad ciudadana es un valor y responsabilidad ineludible del Estado, enmarcada en el cumplimiento de los derechos humanos garantizados constitucionalmente junto con el ordenamiento internacional.

No obstante, para hablar de inseguridad ciudadana, antes también hemos de referirnos a la seguridad como amplio concepto, la seguridad que es, ante todo, un estado de ánimo y como tal, una cualidad intangible, cambiante, mejorable o empeorable por cuestiones puramente derivadas de la afectividad, la sensibilidad, el estado personal y, sobre todo, por la percepción diferente de la información que, en cada momento y circunstancia recibimos y procesamos o emitimos.

Los ciudadanos, cuando oyen hablar de inseguridad ciudadana, piensan en múltiples y muy diversos problemas o situaciones, desde el terrorismo, a la venta de droga en la calle, atracos con armas, violaciones o abusos sexuales, agresiones físicas, robos en domicilios, locales, vehículos, carteras y tirones de bolsos, amenazas, actos de gamberrismo, fraudes, estafas, etc., e incluso recientemente piensan en la corrupción.

Así, la inseguridad ciudadana se ha convertido hace ya tiempo en un desafío crucial para la gobernabilidad democrática y el desarrollo humano. Con todo, a pesar de que en el núcleo de esta inseguridad se halle en la amenaza de violencia generada por los nuevos conflictos producidos socialmente, lo cierto es que las políticas de seguridad ciudadana siguen estando más orientadas a contener o reducir los efectos extremos de estos conflictos (preferentemente la actividad delictiva dirigida contra los bienes privados) que a minimizar los riesgos de exclusión social y de desigualdad económica y, en última instancia, el riesgo de ruptura social en el que cada vez estamos más inmersos.

En resumen, son pues, tiempos de miedo e inseguridad, en los que este discurso público se revela recurrente.

Es momento de apostar con rigor por el desarrollo humano sostenible que, consecuentemente, genera seguridad y es el

requisito imprescindible para poner la "aldea global" en orden.

Todo ello teniendo en cuenta que hoy, la delincuencia organizada y la criminalidad están deteriorando las relaciones sociales y humanas, distorsionando la vida cotidiana y están cambiando incluso conceptos como la solidaridad ante las inseguridades pues el impacto de la violencia y el crimen en el desarrollo es elevado. Por tanto, es necesario seguir profundizando en los conceptos y definiciones sobre Seguridad Humana como holística, que permita dimensionar factores multidimensionales.

Hacia un enfoque integral contra la inseguridad

Como consecuencia de lo anterior, debemos reaccionar contra situaciones de resignación, y dar un cambio decisivo e irreversible hacia un enfoque integral de la seguridad que supongan una continuidad en la reestructuración y modernización de los sistemas policiales y de la justicia para la plena y efectiva coordinación transfronteriza en el combate contra la delincuencia organizada teniendo especialmente en cuenta que la seguridad es, según las encuestas, uno de los aspectos prioritarios para los ciudadanos.

Muestra de ello es que la percepción de inseguridad en los ciudadanos se ha incrementado en los últimos años como consecuencia de, en algunos aspectos, ignorancia por parte de las autoridades o manipulación mediática o difusión de informaciones poco rigurosas.

Basta un ejemplo y es que cuando se le da más tiempo de cobertura mediática a la delincuencia hay un efecto negativo por parte de los medios de comunicación que influye en la percepción del público. Los resultados indican que existe una relación entre el tratamiento informativo de la delincuencia, principalmente, por parte de los canales de televisión, y la sensación de inseguridad.

Reducir las vulnerabilidades

Ante el gran catálogo de riesgos y amenazas de hoy vivimos en un mundo muy vulnerable, aunque como concepto, la vulnerabilidad puede parecer excesivamente amplio y abstracto.

En cualquier caso, la mayoría de las infraestructuras, personas y sociedades, sin importar el nivel de desarrollo cultural, social o económico, son vulnerables en muchos sentidos ante circunstancias y acontecimientos adversos, muchos de los cuales no se pueden predecir ni prever. Somos vulnerables ante las crisis económicas, crisis sanitarias, las amenazas terroristas, los desastres naturales, el cambio climático, los peligros de las actividades industriales, los conflictos o disturbios sociales, las actividades de organizaciones criminales, etc.

Y somos más vulnerables según las capacidades o limitaciones económicas y políticas, ubicación geográfica, niveles de la sociedad, falta de cohesión social o grandes desigualdades, instituciones poco efectivas, gobernanza deficiente, etc.

No obstante, como efecto positivo también de la globalización, la mayoría de los países, en las últimas décadas, están mejorado en cuanto a desarrollo humano y a miles de millones de personas les está yendo mucho mejor, aunque queda mucho por hacer.

Así, el Informe sobre Desarrollo Humano 2013 reveló que más de 40 países en desarrollo (lo que incluye a la mayoría de la población mundial) consiguieron mayores incrementos de desarrollo de lo previsto desde el año 1990.

Aumentar la resiliencia

No obstante, para mejorar nuestras vulnerabilidades, hay que moverse y no sucumbir al miedo ni a la autocomplacencia para aumentar nuestra resiliencia.

Y para aumentar la resiliencia hay que analizar las cuestiones, tendencias y políticas más importantes en materia de desarrollo y seguridad de manera independiente y con base en las evidencias empíricas.

Para reducir las vulnerabilidades y evitar su intensificación, las autoridades y entidades deben implantar soluciones y establecer mecanismos de respuesta adecuados a través de directivas y reglamentaciones para minimizar los riesgos y garantizar que los sistemas respalden el bien común.

Además, en esta globalización, para reducir la vulnerabilidad a amenazas transnacionales, se han de adaptar las estructuras de colaboración internacional para minimizar las crisis, pensando en global para mejor actuar en local mediante la cooperación entre los Estados y en las organizaciones internacionales.

Por contra, la falta de coordinación, cooperación y liderazgo internacional frena el progreso hacia la solución de los problemas globales de seguridad y la reducción de las vulnerabilidades que amenazan el desarrollo humano y, por tanto, requieren de manera sistemática, la transformación armonización de las normas sociales y políticas para un progreso equitativo y sostenible con libertad y seguridad.

El impacto que causa una vulnerabilidad crítica es más que importante y por ello, también hay que aumentar la resiliencia y se requiere algo más que reducir las vulnerabilidades, como eliminar las restricciones a las que se enfrentan los directivos a la hora de actuar con mayor libertad y flexibilidad ante las incidencias.

A lo largo del 2016, la identificación y el análisis de vulnerabilidades serán una pieza importante en los objetivos de la seguridad en las instituciones y empresas y, especialmente, en lo referente a las infraestructuras estratégicas y críticas, que presentan un mayor riesgo.

La definición de las adecuadas políticas de seguridad, la implementación de soluciones globales de seguridad y la adopción de mecanismos que permitan detectar de forma precoz la posible materialización de los riesgos o amenazas y su contraposición con diferentes medidas de seguridad son las principales armas para combatir estas más que potenciales incidencias.

Por todo ello, serán importantes las políticas para reducir las vulnerabilidades y aumentar la resiliencia como: la prevención de las crisis, la promoción incremento de las capacidades, la cohesión y protección social, los acuerdos sobre el cambio climático, la prevención y reducción de los riesgos de desastres naturales, el control de las bandas organizadas y grupos de acción terrorista, etc.

Predicciones de amenazas y tendencias en 2016

Sin grandes dudas, y sobre la base del actual catálogo de riesgos, amenazas y vulnerabilidades, son las infraestructuras críticas y estratégicas las que presentan mayores posibilidades de ataque o incidencias. Los ataques contra este tipo de instalaciones se han incrementado en los últimos años y es esperable que esta tendencia continúe.

Así, hoy múltiples aparatos inteligentes están en situación de riesgo notable. El Internet de las cosas seguirá evolucionando y las entidades y empresas necesitarán proteger de nuevas formas sus dispositivos inteligentes en evolución permanente. Obviamente, los riesgos y amenazas, también.

En este sentido, cabe destacar aspectos como la migración, el terrorismo, la inseguridad ciudadana y las consecuencias del fenómeno de la corrupción. Todo ello en un marco de acción y convivencia global.

Migración

De acuerdo con la ONU, la migración internacional se ha disparado en los últimos años. Hace 25 años se registraban 153 millones de migrantes o refugiados en el mundo, en tanto que, en la actualidad hay 244 millones, un 60 por ciento más *"Y millones han sido convertidos en los chivos expiatorios y en los blancos de políticas xenófobas y de una retórica alarmista",* según recientes declaraciones del Secretario General de la ONU, Ban Ki-moon.

Asimismo, los conflictos y la inestabilidad política han abonado esta migración en forma de refugiados que huyen de las zonas en conflicto. Así, en la actualidad, sólo por el conflicto o cuatro años de guerra en Siria, hay más de 4 millones de refugiados y más de 7 millones de desplazados.

"Debemos recordar que aquellos que cometen actos de terrorismo quieren que estemos asustados. Si caemos en esta trampa, ellos habrán triunfado", son las recientes palabras igualmente de Ban Ki-moon que aseguró que precisamos nuevos esfuerzos con urgencia e instó a crear un nuevo pacto global sobre la movilidad humana basado en una mejor cooperación entre los países de origen, de tránsito y destino.

Es por tanto urgente la inclusión de los excluidos en el escenario actual por justicia y protección y porque, consecuentemente, aumenta la inseguridad global y local de los países implicados o afectados.

Terrorismo

Aún cuando los conflictos y las guerras asimétricas no acabarán nunca, lejos de su pronta resolución estamos, si cabe, en graves momentos de riesgo y amenazas a la seguridad global, además de aquellas áreas de conflicto.

Salvo excepciones, los conflictos simplemente se están trasladando de un lugar a otro. Un flujo de siniestros intereses políticos y económicos parece estar en el ambiente. Lo sucedido, especialmente destacado en Nueva York, Madrid, Londres, Bruselas y este último año en París, ha puesto en evidencia que vivíamos en un orden social sustentado en la confianza y la autocomplacencia y que, esos hechos consumados que son los actos terroristas, son consecuencia del hecho premeditado del terrorismo y la percepción del potencial negativo del impacto social que genera.

Unos conflictos armados y guerras asimétricas que se inician con la intervención en Irak, incomprensible aventura de la historia moderna, justificada tras los atentados de Nueva York y Washington, donde el gobierno estadounidense, con el apoyo de una amplia mayoría de la comunidad internacional, decidió bombardear Afganistán, refugio de Bin Laden y que, como se ha dicho hasta la saciedad, no colmaba su sed de venganza y así continúa.

Llegados a este punto, es necesario no perder el referente de que los costes de estas guerras asimétricas siguen aumentando de manera espectacular y sus "beneficios directos" se han ido reduciendo, por lo que, actualmente, solo tenemos conflictos allí donde la riqueza material es objetivo de botín a repartir, como son las materias primas y los combustibles fósiles.

Con el inicio en una guerra no querida, la de Irak; un conflicto soportado, el de Siria; y unos ataques importados, los de los países europeos, la historia continúa con cada vez mayor amenaza y sufrimiento del terrorismo yihadista.

Inseguridad ciudadana y corrupción

Aunque es cierto que, en general, los países de la Unión Europea tienen indicadores de criminalidad sostenibles, distintos países, principalmente latinoamericanos, presentan cifras de homicidios superiores a las de naciones en conflicto armado.

Estas cifras han llevado a la Organización Mundial de la Salud a calificar los homicidios en Latinoamérica como una "epidemia" –más de 10 asesinatos por 100.000 habitantes- y tendencia en la región a convertirse en la más insegura del mundo, de acuerdo a datos del Banco Mundial. Y lo que es más grave, es que más allá del trauma y sufrimiento, el crimen y la violencia no sólo conlleva costes sociales económicos desorbitados que van desde el 3% del PIB en Chile y Uruguay, hasta más del 10% del PIB en Honduras, sino que organizaciones criminales ya actúan transfronterizas, incluso situándose en países europeos.

Pero, también la corrupción está generando inseguridad ciudadana pues vivimos momentos de especial impacto, tanto en la realidad como en la percepción ciudadana, sobre la inseguridad que están provocando los elevados niveles de corrupción que, aunque esta se pueda entender como un fenómeno nocivo, vasto, diverso y global cuyos protagonistas pertenecen tanto al sector público como al ámbito privado, está llevando a momentos de indignación y protesta cercanos al movimiento ciudadano.

Una corrupción que no se refiere al simple saqueo de recursos del Estado sino que incluye el ofrecimiento y la recepción de sobornos; la malversación y la negligente asignación de fondos y gastos públicos; la manipulación de precios; los escándalos políticos o financieros; el tráfico de influencias e información privilegiada; la financiación ilegal de partidos políticos; la parcialidad o dudosas decisiones judiciales; el amiguismo o sueldos exagerados de amistades, a pesar de su incapacidad; los concursos amañados sobre obras o servicios o la indebida calificación de las mismas; la compra de equipamiento de mala calidad o encarecidos, etc.

Todo ello genera consecuencias significativas pues la corrupción reduce la eficiencia del gasto público. La corrupción distorsiona la estructura del aparato productivo pues su incidencia está basada en las decisiones administrativas sobre recalificaciones, permisos, etc. La corrupción desalienta al contribuyente pues la eficacia del sistema recaudatorio se asienta sobre un conjunto de condiciones, incluida la conciencia social que consigue que los ciudadanos acepten como un deber contribuir al esfuerzo común. Finalmente, la corrupción deteriora los organismos de control y ello genera también inseguridad al ciudadano.

Con este panorama y a modo de conclusiones, podemos decir que, con respecto a la seguridad global y local, la actual sociedad requiere de un punto de vista nuevo y diferenciador y una determinada manera de entender el tiempo, que es más corto y el espacio, que es más grande, de la mano de la lógica, la inseguridad y la causalidad, que son invitados permanentes.

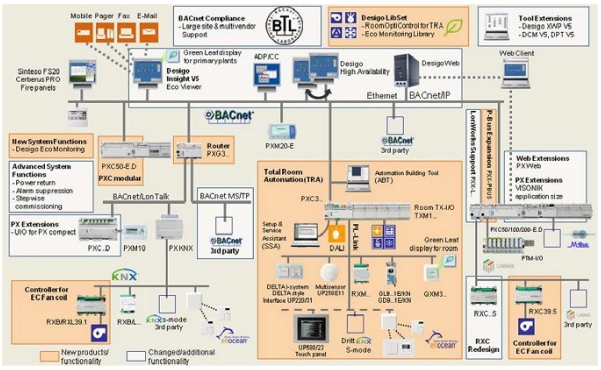
Así consecuentemente, en el año 2016 requerimos, y es de especial responsabilidad, seguir avanzando en el cambio de paradigmas de seguridad, imprescindibles para acometer nuevos retos y exigencias de la sociedad en que vivimos. Hemos de analizar y actuar sobre aspectos de seguridad con una visión holística, pues el mundo no está formado por piezas separadas y aisladas, sino conjuntos que guardan una relación compleja y sinérgica entre sí. Y hemos de seguir avanzando en global para mejor actuar en nuestra dimensión local y ciudadana.

BMS: Edificios inteligentes, ¿y seguros?

Instituto Nacional de Ciberseguridad

Los Sistemas de Gestión de Edificios (BMS - Building Management System), desde su aparición a finales de los años 70 hasta la actualidad, han sufrido una gran evolución, al igual que el resto de sistemas de control.

Un BMS moderno se basa en la integración de una serie de subsistemas que, en general, comparten una infraestructura como: base de datos, central de alarmas y otros subsistemas específicos como el control de la iluminación o la climatización. La figura inferior refleja la topología de un BMS complejo, con sistemas dedicados e independientes para la iluminación, climatización y control de accesos que comparten una infraestructura de integración. Así se puede observar la presencia de los correspondientes protocolos que operan en las distintas áreas de gestión como iluminación (DALI), climatización (BACNet), etc.



A la hora de considerar el diseño de un sistema BMS es de gran importancia conocer las funcionalidades a cubrir en el entorno de aplicación. En este contexto, conviene no confundir sistemas BMS orientados a edificios terciarios (vertiente industrial) con BMS orientados a viviendas familiares (vertiente domótica). En ambos campos se pueden encontrar sistemas equivalentes pero con diferencias que pueden trasformar un caso de éxito en un rotundo fracaso.

En sistemas más pequeños, como las edificaciones privadas y hogares, se colocaba un PLC de pocas entradas/salidas para dar soporte a la climatización, iluminación y otros aspectos a controlar. Hoy en día, esta idea evoluciona hacia la implantación de elementos independientes basados en sensores de control, que mediante Ethernet mandan mensajes que son visualizados en una tableta o similar; es decir, se aprecia una evolución de los sistemas BMS hacia un subconjunto del paradigma IoT (Internet of Things).

La tecnología base de los sistemas de control de los sistemas BMS es similar a los sistemas basados en equipos PLC más tradicionales como las empleadas en el sector eléctrico. Lo que realmente diferencia este entorno de otros es la adecuación de los sistemas de control hacia los protocolos utilizados para comunicar los dispositivos entre sí y con los servidores.

Protocolos empleados en gestión de edificios

Dentro de un BMS existen multitud de protocolos, algunos de ellos específicos de este campo de aplicación y otros más generalistas. Entre los protocolos de comunicaciones especializados podríamos destacar DALI, para la gestión de la iluminación, o BACNet, usado en la gestión de sistemas de climatización. A su vez, entre los protocolo más generales se puede citar a KNX, LonWorks o ModBUS. Quizá debido a su sencillez, este último es implementado por gran cantidad de fabricantes de BMS y se ha convertido de facto en uno de los estándares más comunes.

Muchos de estos protocolos son muy antiguos y en el momento de su nacimiento la seguridad no era una de las prioridades de diseño. Hoy en día, es necesario que se incluyan mejoras de seguridad para los protocolos utilizados, como puede ser el cifrado o la autenticación, y que sean interoperables. Estas mejoras ya se están incorporando actualmente.

A la serie de protocolos citados anteriormente se ha unido en los últimos años una extensa familia de protocolos inalámbricos de nueva generación (ZigBee, Wifi, EnOCEAN,...), que pugnan por erigirse como el dominante en este sector. Los protocolos inalámbricos implementan mayores niveles de seguridad, que disminuyen sus amenazas frente a ataques externos, pero carecen de la fiabilidad, (en términos de alta disponibilidad, latencia, etc.) de sus homólogos por cable.

Seguridad de los protocolos más característicos en BMS

BACnet

La arquitectura de seguridad del protocolo BACnet es opcional dentro del despliegue BACnet. La seguridad en BACnet provee paridad en las entidades, asociación de datos en origen así como autenticación, confidencialidad e integridad.

La seguridad de este protocolo se basa en el despliegue de pares de claves. Existen seis tipos de pares de claves: los que permiten el acceso a la red general, los que autentican a los usuarios, los específicos de la aplicación, los utilizados para la instalación, los empleados para la distribución y los maestros.

Además BACnet proporciona una especificación extensa para:

- Proporcionar seguridad a los mensajes enviados: Introduce una cabecera de seguridad a nivel de mensaje APDU de BACnet.

- Implementar políticas de seguridad de red: Existen dos tipos de redes, las confiables (aquellas que bien físicamente o bien por su cifrado lo son) y las no confiables. Teniendo en cuenta esto, BACnet considera cuatro tipos de políticas de seguridad en red:

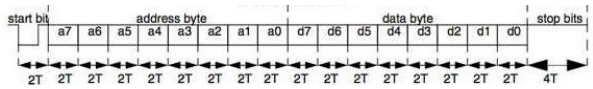
  - Confiable-texto en plano: requiere seguridad física de la red pero no la del propio protocolo.
  - Confiable-firmado: no se requiere la protección física, la seguridad está dada por el firmado que permite el protocolo.
  - Confiable-cifrado: sin protección física, seguridad por cifrado.
  - No Confiable-texto en plano: sin seguridad alguna.

- Proporcionar un nivel de seguridad del dispositivo BACnet: asegura a niveles de seguridad según la política BACnet independientemente de si se sitúa en redes seguras o inseguras.

- Proveer la autenticación de usuario: mediante la provisión de claves de usuario.

DALI

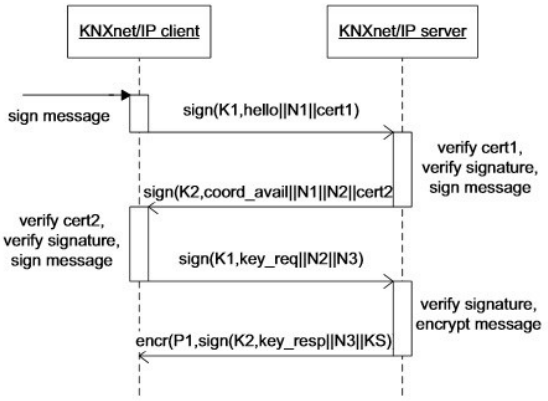
El protocolo DALI (Digital Addressing Lightning Interface) es ampliamente utilizado en BMS para la gestión de iluminación. Es un protocolo muy sencillo. El siguiente gráfico muestra la trama de datos del protocolo. Obsérvese que únicamente hace uso de dos campos que identifican el destino (address) y la instrucción (data).



DALI no incorpora ninguna medida de seguridad transmitiéndose los datos en claro a través del bus de comunicaciones. Este es un ejemplo de característica propia de un protocolo BMS que es necesario tener en cuenta en su despliegue, asegurando la incorporación de mecanismos adicionales que contrarresten el riesgo que supondría el acceso a esta información.

KNX

La extensión EIBsec de KNX provee los mecanismos de seguridad a nivel de aplicación para las tramas KNXnet. La capa de seguridad se asienta sobre los protocolos TCP o UDP. Para que un dispositivo se comunique de forma segura con este protocolo debe:



- Crear los certificados: usando una autoridad de certificación con el ETS (Engineering Tool Software), firmando las claves públicas de los dispositivos comunicándose con KNX.

- Distribuir los pares de claves. Los dispositivos KNX pueden autenticarse entre ellos tanto de forma unicast como multicast.

- Establecer una comunicación segura mediante claves simétricas (por agilidad también para los casos multicast).

LonWorks

Lonworks es un protocolo proveniente de los fabricantes de climatización para controlar sus sistemas.

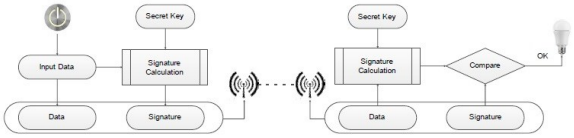
El protocolo se diseñó para ser utilizado con dispositivos de capacidad muy limitada (CPU de 8 bits utilizando 200 bits de procesamiento para datos), por ello es importante elegir algoritmos de cifrado adecuados para este tipo de dispositivos. El tiempo necesario para procesar algoritmos asimétricos puede llegar a emplear hasta 83 segundos para descifrar RSA por ejemplo. Por ello es imperativo el uso de algoritmos simétricos, como 3DES o AES de 128 bits, que requieren de menor coste computacional y por tanto menos tiempo, con sus bondades y debilidades.

Los servicios definidos en el protocolos están disponibles para comunicación tanto unicast como multicast.

EnOCEAN

EnOCEAN es un protocolo privativo de uso extendido en los BMS para las aplicaciones de captación de energía. Los equipos (sensores y dispositivos) se han diseñado para transmitir su información de estado y control a través de radio.

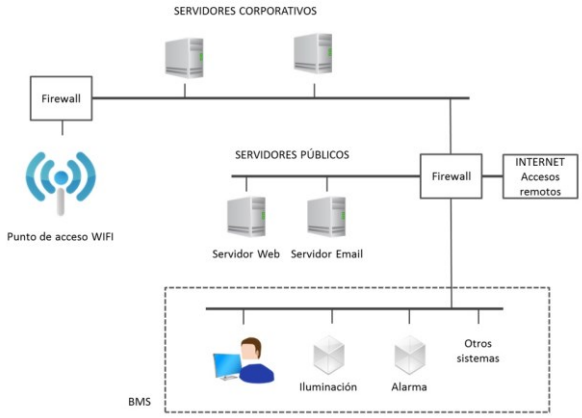
En el año 2012, se introdujeron los primeros mecanismos de seguridad en la API de EnOCEAN. El protocolo utiliza un cifrado para la autenticación a nivel MAC. Permite una función dinámica de cambiar la clave con un contador (vulnerable si el contador o el diferencial son débiles).



Otros aspectos genéricos de seguridad

En los sistemas utilizados en edificios inteligentes, además de escoger y configurar cuidadosamente un protocolo de control adecuado, deben contemplarse las medidas de seguridad habituales como es el control de usuarios, uso de cortafuegos, accesos remotos por VPN, etc. En cuanto a topología de red se refiere, puede optarse por un diseño de red segmentado como, el representado en la siguiente figura:

Los mecanismos de seguridad que puedan aportar protocolos específicos de control, en ocasiones quedan invalidados por la no observación de otras medidas genéricas en sistemas informatizados.



En este sentido, la realidad es que, todavía muchos de los sistemas BMS existentes no aplican estas recomendaciones de seguridad globales y es común encontrar, por ejemplo, conexiones expuestas y accesibles de forma abierta desde Internet.

Por ello no hay que olvidar que, además de implantar la seguridad a nivel de protocolo, es importante aplicar las medidas genéricas habituales de protección de sistemas: políticas de contraseñas, segmentación de red apropiada, bastionado de equipos, así como controlar la información proporcionada por el sistema. Con esto, el esfuerzo de toda la industria que rodea la implantación y desarrollo de BMS sí concluye en una aproximación segura de toda la tecnología disponible.

Fuente: Instituto Nacional de Ciberseguridad

Posibilidades de investigación de la identidad de usuarios de internet

Jesús Valladares
Socio Fundador de Avezalia, firma especializada en el asesoramiento jurídico integral TIC

A todos los que nos dedicamos al derecho relacionado con las nuevas tecnologías y a muchos usuarios se nos ha planteado alguna vez la misma cuestión: ¿en qué medida es posible la investigación de la identidad de una persona que, abusando del supuesto anonimato que proporciona Internet, comete delitos empleando la red? ¿Es posible su identificación en todo caso? ¿Cómo se persigue a este tipo de delincuentes?

Punto de partida

El punto del que partimos es el de aquel sujeto que, amparándose en el supuesto anonimato que proporciona la red, emplea la misma para cometer un delito. Su intención no es otra que la entorpecer, en la medida de lo posible, su identificación y, con ello, su responsabilidad penal y civil.

¿Qué medios tenemos para averiguar su identidad?

Partiendo de que hay servicios que no requieren registro previo de usuario y de que hay otros que, si bien lo exigen, no pueden corroborar la veracidad de los datos ofrecidos por el usuario en el procedimiento de alta, el dato más idóneo de que disponemos es el de la dirección IP que emplea el delincuente para conectarse al servicio en el que comete el delito.

Es, precisamente, este dato de la dirección IP el que puede vincular al delincuente con una persona de carne y hueso a la que poder llevar ante los tribunales.

¿Cómo conseguimos la identidad que hay tras una dirección IP?

La vinculación identidad - dirección IP que pretendemos la podemos conseguir de los operadores de servicios de telecomunicaciones, ya que son los encargados de proveer tales direcciones a los sujetos usuarios de las redes.

Es algo tan fácil como ir a una compañía de telecomunicaciones tipo Movistar, Vodafone y Orange y dar de alta una línea de datos que te permita conectarte a internet. Dicha conexión se efectúa por medio de una dirección IP.

¿Dónde se regula la forma de proveer la información del titular de una dirección IP?

1.- Ley 25/2007, de 18 de octubre de 2007, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Esta primera norma, según su artículo 1º, tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación (excluyendo el contenido de las mismas) y la de cederlos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves.

Por tanto, parece que esta norma sólo parece autorizar la realización de actuaciones de investigación para la averiguación de la identidad de aquellos usuarios que actúen con seudónimo a través de redes de comunicaciones en caso de comisión de delitos graves.

2.- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
Esta segunda normal señala que los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo dispuesto en la Ley de Enjuiciamiento Criminal y añade que los sujetos obligados han de facilitar los datos indicados en la orden de interceptación legal, especificando que la identidad o identidades del sujeto objeto de la medida de interceptación sería uno de esos datos a facilitar, así como la identidad o identidades de otras personas involucradas en la comunicación electrónica.

No obstante, esta norma no hace referencia alguna a la gravedad del delito que se investiga, limitándose a remitirse a lo dispuesto en la Ley de Enjuiciamiento Criminal.

¿Qué nos dice la jurisprudencia?

A la vista de este panorama normativo, han venido dictándose pronunciamientos jurisprudenciales totalmente contradictorios:

1.- Jurisprudencia restrictiva.
En unos casos se han basado, exclusivamente, en lo dispuesto en la Ley 25/2007 y, dentro del mismo, en considerar como delitos graves aquellos que, exclusivamente, tengan una pena superior a 5 años.

2.- Jurisprudencia más abierta

En otros casos, también ha existido jurisprudencia de nuestros tribunales que, amparándose en la actual normativa y en la jurisprudencia del Tribunal Constitucional acerca de la posibilidad de limitar derechos fundamentales con la finalidad de esclarecer conductas delictivas, ha venido estimando la realización de actuaciones de investigación para la averiguación de la identidad de aquellos usuarios que actúen con seudónimo a través de redes de comunicaciones.

Razones de política criminal para mantener una postura amplia en la averiguación de la identidad de usuarios de Internet en caso de comisión de delitos

La no atención a las medidas de investigación como las que se proponen en el presente post, impediría la investigación tecnológica de delitos que, frecuentemente, utilizan las redes de comunicación para su comisión, pero que no tienen la consideración de graves al tener asociada una pena abstracta inferior a 5 años, (por ejemplo, el delito de posesión, producción, venta o difusión de material pornográfico en que se hayan utilizado menores de edad o el delito de favorecimiento de la prostitución de menores de edad).

Del mismo modo, se mandaría un mensaje claro a la ciudadanía: barra libre en Internet para delinquir cuando la pena asociada al delito, en abstracto, sea inferior a 5 años, con el consiguiente fracaso de los fines preventivos que su tipificación penal persigue.

Argumentos legales y jurisprudenciales a favor de la investigación de la identidad de usuarios de internet en caso de comisión de delitos

Es cierto que la Ley 25/2007, como vimos anteriormente, hace una referencia expresa a la persecución de delitos graves, pero no es menos cierto que dicha norma no ha establecido que la determinación de los delitos graves lo deba ser sobre la base, en exclusiva, de la gravedad de las penas que, en abstracto, lleven aparejadas dichos delitos.

De hecho, tal limitación sería la única de nuestra legislación que utiliza dicho parámetro de valoración como elemento inamovible del juicio de proporcionalidad en la limitación de derechos fundamentales.

Por tanto, corresponde a la jurisprudencia realizar tal determinación atendiendo a las pautas usuales de interpretación normativa.

En coherencia con ello, la Jurisprudencia constitucional, a la hora de valorar la procedencia de adoptar medidas restrictivas del derecho fundamental al secreto de las comunicaciones, ha venido desarrollando un juicio de proporcionalidad que ha de llevarse a cabo antes de acordar la limitación del derecho, atendiendo a criterios tales como:

- La importancia y relevancia social del bien jurídico protegido
- La trascendencia social de los efectos que el delito genera
- El hecho de que el delito a investigar sea cometido por organizaciones criminales
- La dificultad o imposibilidad de su persecución a través de otras medidas menos gravosas para los derechos fundamentales en litigio
- El beneficio obtenido mediante la medida, que ha de ser mayor que el coste que el sacrificio comporta.

En apoyo de dicha valoración jurisprudencial, hay que resaltar que la propia Ley 25/2007 excluye de su ámbito el núcleo esencial del derecho al secreto de las comunicaciones, esto es, el "contenido" de las comunicaciones electrónicas, para cuya interceptación no se establece expresa limitación legal en función de la gravedad penológica del delito, como resulta del artículo 39 de la Ley 9/2014 y de lo dispuesto en el artículo 579 de la LeCrim.

Conclusiones

En base a todo lo anterior, podemos concluir que no existe base suficiente para entender que la Ley 25/2007 haya fijado la gravedad del delito tomando como exclusivo parámetro la pena legalmente prevista para el mismo y que, en consecuencia, establezca una prohibición de utilizar la investigación tecnológica para todo delito cuya pena no supere en su previsión abstracta los cinco años de prisión, cualesquiera que sean el resto de circunstancias concurrentes.

Por tanto, han de incluirse otros delitos castigados con pena inferior y que, por tanto, tienen la calificación legal de "delitos menos graves", pero que merecen la consideración de graves en atención a parámetros tales como la importancia del bien jurídico protegido, la trascendencia social de los efectos que el delito genera o la inexistencia de medios alternativos, menos gravosos, que permitan su investigación y esclarecimiento.

Fuente: Legal Today

Servicio nocturno en Centro Comercial

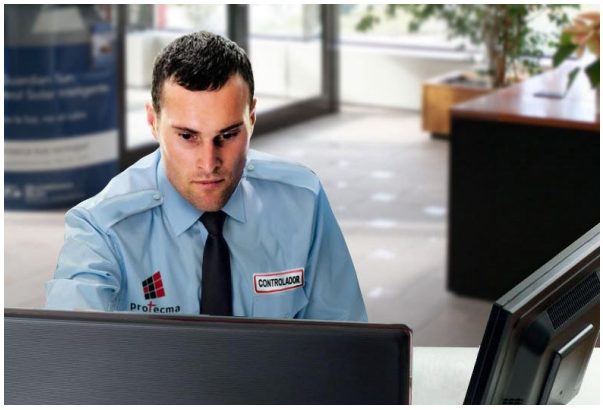
Unidad Central de Seguridad Privada

ANTECEDENTES

El presente informe se emite a petición de una Administración de Fincas, en la que viene a consultar, si un servicio nocturno en un Centro Comercial, tiene que ser prestado por un vigilante de seguridad, o por un conserje.

CONSIDERACIONES

Con carácter previo se participa que, los informes o respuestas que emite esta Unidad, tienen un carácter meramente informativo y orientativo -nunca vinculante- para quien los emite y para quien los solicita, sin que quepa atribuir a los mismos otros efectos o aplicaciones distintos del mero cumplimiento del deber de servicio a los ciudadanos.



La consulta planteada, guarda relación con un servicio nocturno, en un Centro Comercial, cuando se encuentra cerrado al público, donde el personal que se contrate, sea Conserje o Vigilante de Seguridad, tendría como actividades a realizar: la limpieza del Centro Comercial, y la apertura de puertas a personas que tengan relación profesional con las instalaciones del establecimiento comercial.

La Ley de Seguridad Privada 5/2014, en su artículo 32, viene a recoger las funciones de los vigilantes de seguridad, y entre otras, se enumeran las siguientes:

"1. Los vigilantes de seguridad desempeñarán las siguientes funciones:

a) Ejercer la vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto privados como públicos, así como la protección de las personas que puedan encontrarse en los mismos, llevando a cabo las comprobaciones, registros y prevenciones necesarias para el cumplimiento de su misión.

b) Efectuar controles de identidad, de objetos personales, paquetería, mercancías o vehículos, incluido el interior de éstos, en el acceso o en el interior de inmuebles o propiedades donde presten servicio, sin que, en ningún caso, puedan retener la documentación personal, pero sí impedir el acceso a dichos inmuebles o propiedades. La negativa a exhibir la identificación o a permitir el control de los objetos personales, de paquetería, mercancía o del vehículo facultará para impedir a los particulares el acceso o para ordenarles el abandono del inmueble o propiedad objeto de su protección.

c) Evitar la comisión de actos delictivos o infracciones administrativas en relación con el objeto de su protección, realizando las comprobaciones necesarias para prevenirlos o impedir su consumación, debiendo oponerse a los mismos e intervenir cuando presenciaren la comisión de algún tipo de infracción o fuere precisa su ayuda por razones humanitarias o de urgencia.

d) En relación con el objeto de su protección o de su actuación, detener y poner inmediatamente a disposición de las Fuerzas y Cuerpos de Seguridad competentes a los delincuentes y los instrumentos, efectos y pruebas de los delitos, así como denunciar a quienes cometan infracciones administrativas. No podrán proceder al interrogatorio de aquéllos, si bien no se considerará como tal la anotación de sus datos personales para su comunicación a las autoridades.

Lo dispuesto en el párrafo anterior se entiende sin perjuicio de los supuestos en los que la Ley de Enjuiciamiento Criminal permite a cualquier persona practicar la detención."

El apartado 2, del mismo artículo 32 de la Ley de Seguridad Privada, clarifica la cuestión al establecer lo siguiente:

"2. Los vigilantes de seguridad se dedicarán exclusivamente a las funciones de seguridad propias, no pudiendo simultanearlas con otras no directamente relacionadas con aquéllas."

Respecto a las actividades complementarias, que pueden realizar los vigilantes de seguridad, el artículo 70.1) del vigente Reglamento de Seguridad Privada establece que:

"No se considerará excluida de la función de seguridad, propia de los vigilantes, la realización de actividades complementarias, directamente relacionadas con aquélla e imprescindibles para su efectividad".

CONCLUSIONES

A tenor de lo recogido en los artículos 32 y 41, de la Ley 5/2014, de Seguridad Privada, en concordancia con el artículo 5.1.a) de la misma ley, los servicios de vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto públicos como privados, así como de las personas que pudieran encontrarse en los mismos, se ha de prestar por Vigilantes de Seguridad o, en su caso, por Guardas Rurales, cuando la finalidad sea la de proteger, prevenir o evitar la posible comisión de actos dañinos o delictivos. Igualmente contempla que los vigilantes de seguridad se dedicarán exclusivamente a las funciones de seguridad propias, no pudiendo simultanearlas con otras no directamente relacionadas con aquéllas.

Según lo indicado en el escrito de consulta, en el Centro Comercial, el horario de prestación de la actividad seria nocturno, por lo que se puede entender que, en buena lógica, la vigilancia nocturna ha de estar reservada al personal de seguridad privada, por cuanto en tales circunstancias podrían requerirse potestades específicas en orden a la represión de posibles agresiones a la seguridad de los bienes y personas.

A la vista de lo expuesto, la acción de limpiar el Centro Comercial, se considera excluida de las propias de vigilancia y protección de un servicio de seguridad privada, y por tanto no cabe su realización por el Vigilante de Seguridad, puesto que en sí, no parece que complete o perfeccione la dinámica del mismo. Dicho lo anterior, la apertura de puertas en horario no comercial, a personas que guardan relación con la actividad de las instalaciones, se podría considerar como actividad complementaria, y por tanto en momentos puntuales realizables por los vigilantes de seguridad.

Este informe se emite en cumplimiento de lo dispuesto en el artículo 35.g) de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, sobre derecho de información al ciudadano, y fija la posición y el criterio decisor de las Unidades Policiales de Seguridad Privada, en relación con el objeto de la consulta sometido a consideración. No pone fin a la vía administrativa ni constituye un acto de los descritos en el artículo 107 de la citada ley, por lo que, contra el mismo, no cabe recurso alguno.

Tú casa inteligente ¿es cibersegura?

Oficina de Seguridad del Internauta

Tu casa inteligente está conectada, y por tanto, no se libra de posibles ataques cibernéticos. Conoce cuáles podrían ser algunos de sus talones de Aquiles y como podría afectarte.

¿Te has imaginado alguna vez como sería tu casa si todos los elementos que la componen estuviesen conectados? La televisión, el frigorífico, el sistema de iluminación, la calefacción… Hace unos años parecía una cosa de locos el simple hecho de pensarlo. Sin embargo, a día de hoy, a nadie le sorprende que esto pueda ser posible, ¿será porque el "Internet de las cosas" ha llegado para quedarse? Sí, has oído bien, el Internet de las cosas, el escenario en el que cada vez más objetos están conectados y diseñados para recopilar, intercambiar y procesar datos con el fin de mejorar nuestra calidad de vida.

Algunos de nosotros ya disponemos en nuestra casa de algún objeto que puede ser programado y controlado con el smartphone o tablet. Por poner algún ejemplo, la última versión de los famosos aspiradores Roomba de iRobot, no solo es capaz de aspirar toda la casa de forma autónoma sino que además, gracias a una app que sus fabricantes ponen a nuestra disposición podemos controlar la aspiradora desde el móvil. También hay robots de cocina que pueden ser sincronizados con smartphones y tablets y frigoríficos que permiten tener bajo control qué alimentos almacenamos, qué recetas se pueden hacer con dichos alimentos, cuales necesitamos comprar o incluso saber la fecha de caducidad. Los electrodomésticos que hemos mencionado son solo una pequeña parte de todo lo que podemos encontrar en el mercado. Interesante ¿verdad?

Ventajas vs inconvenientes

Todo parecen ventajas cuando hablamos de casas inteligentes: mejoran las tradicionales funcionalidades, simplifican su uso y mantenimiento, permiten ser manejadas desde cualquier lugar a cualquier hora, etc. Sin embargo, como cualquier otro dispositivo que permite ser conectado a Internet (ordenador, smartphone, tablet, wearable, etc.) no está exento de riesgos de seguridad y privacidad y por tanto, debemos tener controlados o por lo menos, ser conocedores de ellos para garantizar así la protección de las personas que vivimos o visitamos un determinado hogar.

El rápido desarrollo de los dispositivos inteligentes por parte de los fabricantes, empleando esfuerzos principalmente en diseño y funcionalidad provoca que se invierta menos en aspectos de seguridad, aun sabiendo que esto pueda ser un error, o de hacerlo, la complejidad del desarrollo del producto dificulta garantizar una seguridad del 100%. Como consecuencia de esto, los ciberdelincuentes se ven motivados a buscar vulnerabilidades y en caso de encontrarlas, se encargan de hacerlas públicas en el mejor de los casos, aunque pudiera ser también que se dedicaran a poner en circulación amenazas capaces de explotarlas.

Por tanto, ¿a qué riesgos podríamos estar expuestos?

Una buena forma de entenderlos es con situaciones reales que se podrían producir. Leed con atención:

- **Inutilización del dispositivo**

Si un atacante consigue acceder a nuestra conexión de Internet, podría infectar el dispositivo objeto del ataque con malware o enviar órdenes para inutilizarlo o provocar que no funcione correctamente. Esto sucedió por ejemplo con una SmartTV de Samsung.

- **Perjuicio económico**

Si consiguen controlar el sistema de iluminación de la casa o los termostatos de la calefacción, es fácil suponer que podrían encenderlos o elevarlos mientras no estemos en casa incrementando el gasto de las facturas mensuales si nosotros ser conscientes de cuál es la causa del incremento del consumo.

- **Pérdida de privacidad**

Los sistemas inteligentes pueden llegar a almacenar mucha información sobre nosotros: datos personales, gustos, preferencias, estados de ánimo, estilo de vida… Si consiguen acceder a toda esa información, nuestra

privacidad se puede ver claramente expuesta provocándonos problemas psicológicos, familiares, laborales, etc.

- **Robo o secuestro**

Imaginaros que consiguen acceder a las cámaras de seguridad de vuestra casa para saber cuándo estáis ausentes, desactivar los detectores de movimiento y/o abrir la puerta de entrada a la vivienda. Los ladrones podrían entrar en nuestra casa tranquilamente sin despeinarse.

- **Problemas para la salud**

En el Internet de las cosas, los problemas de salud podrían producirse por la explotación de fallos de seguridad en el software o hardware de un marcapasos, máquinas de diálisis o cualquier otro aparato o dispositivos de estas características que afectan directamente a nuestro estado de salud. Dejando de lado éstos, que obviamente son un riesgo para la salud, pero que no se consideran elementos de una casa inteligente como tal, hay otros sistemas que sí se enmarcan dentro de las casas inteligentes y que pueden suponer un riesgo para la salud. Por ejemplo, si consiguen desactivar los detectores de gas y se produce un escape, podríamos intoxicarnos, o si inhabilitan un termostato en plena ola de frio, podríamos coger un resfriado.

- **Participación en actividades ilícitas**

Si un ciberdelincuente utiliza uno de nuestros electrodomésticos, como puede ser el frigorífico, para participar en actividades delictivas, podría meternos en problemas. Nos referimos a situaciones como: alojamiento de contenido ilegal, distribución de malware o robo de información entre otros. Si nos vemos implicados en una situación de estas características, deberemos defender nuestra inocencia en caso de problemas… ¿No os creéis que esto pueda ser posible? Pues parece que sí, al menos hay una nevera responsable de una botnet.

Ahora que ya nos hacemos una idea de los riesgos a los que podríamos estar expuestos si “conectamos” nuestra casa, ¿qué podemos hacer? Como usuarios y hasta la fecha, poca cosa, ya que no tenemos muchas armas para defendernos: deficientes configuraciones de privacidad y seguridad, almacenamiento de datos y comunicaciones con otros dispositivos sin cifrar, falta de herramientas de protección… El primer paso lo deberían dar los fabricantes, sacando al mercado productos seguros, con un ciclo de vida continuo en el que un sistema de actualizaciones sea capaz de corregir problemas que puedan ir apareciendo a lo largo del tiempo. Nosotros como usuarios, trataremos de aplicar las recomendaciones que siempre os damos para proteger vuestros dispositivos:

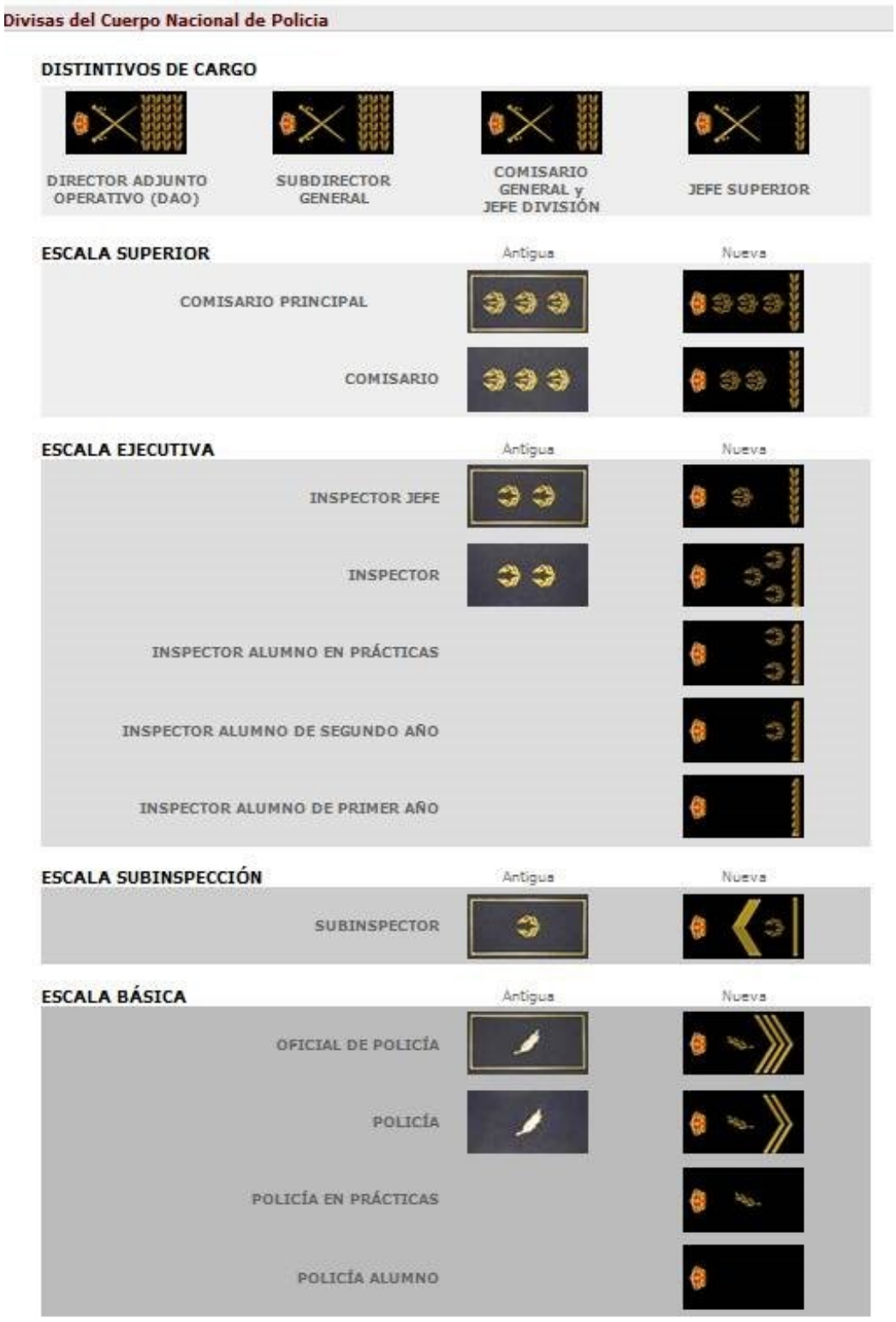
- Valorar la seguridad del dispositivo además de sus características técnicas.
- **Revisar y configurar las opciones de privacidad y seguridad** para marcar o desmarcar, lo que corresponda en cada caso, las casillas que den permisos para realizar ciertas acciones que no deseemos.
- **Mantenerse informados sobre las posibles actualizaciones del software.** En caso de existir una, instalarla lo antes posible.
- En caso de que exista, **instalar alguna herramienta de protección.**
- **Configurar correctamente la conexión wifi de casa** a la que se conectarán vuestros dispositivos inteligentes.
- **Realizar búsquedas** para saber qué opinión tienen otros usuarios sobre ese dispositivo inteligente en concreto.

En cualquier caso, el futuro del Internet de las cosas es verdaderamente prometedor y debemos aprovecharnos de todas las posibilidades que nos ofrece. Simplemente como usuarios, debemos ser cautos y poner en una balanza, al igual que hacemos con otros aspectos de la vida, las ventajas que nos ofrece frente a los inconvenientes y decantarnos de esta forma, por la opción de “conectar” la lavadora, sistema de electricidad o ventilación con nuestros dispositivos o no.

Fuente: Oficina de Seguridad del Internauta

Noticias

Nuevas divisas del Cuerpo Nacional de Policía



Formación

I Congreso Nacional de Formación Reglada en Seguridad Privada

- Días: Del 9 al 11 de Marzo
- Lugar: Ourense

Bajo el lema "***Cultura de seguridad, Formación e Información. Un proyecto compartido***", este Congreso es el punto de partida para definir la hoja de ruta del futuro de la formación en el sector, tanto en lo referente a la Formación Profesional del personal Operativo, como de la Universitaria en los Directores y Jefes de Seguridad, así como de los Detectives Privados.

La Asociación organizadora del encuentro tiene entre sus principales objetivos la promoción y mejora de la imagen del sector de la seguridad privada a través de la mayor y mejor cualificación posible de sus profesionales.

Todos sabemos que el sector de la Seguridad Privada demanda, cada vez más, soluciones eficaces en la formación. El Congreso quiere ser un **punto de encuentro** con el objetivo primordial de buscar el apoyo de los profesionales docentes en este sector, involucrados mediante sus ideas, opiniones y propuestas en pro de la dignificación y profesionalización de un sector que genera cada día más puestos de trabajo; de un sector con un gran futuro por delante.

Adjuntamos dossier presentación del congreso

Cursos 100% online y homologados por el Ministerio del Interior (Resolución 2014) para obtener la habilitación de Director de Seguridad.

Certificados por el Instituto Universitario Gutiérrez Mellado de la Universidad Nacional de Educación a Distancia -UNED-

Claustro con más de 30 profesores, expertos en cada una de las materias del curso.

Los interesados podrán obtener la **habilitación** profesional como **Director de Seguridad** (Ministerio del Interior), con la opción adicional de acceder a la **especialización** para desarrollar e implantar **Proyectos y Planes de Protección en Infraestructuras Críticas**.

Unico curso que ofrece la posibilidad de habilitarse como Director de Seguridad y adquirir los conocimientos necesarios para responder a las necesidades y nuevos retos y exigencias, crecientes e irreversibles que plantea la Seguridad en Infraestructuras Críticas y Estratégicas.

Más información en el siguiente enlace

Planes de carrera para Directores de Seguridad Privada

Oferta formativa de la Escuela de Prevención y Seguridad Integral

Más información en el siguiente enlace

Foment Formació (Cursos Masters y Píldoras Formativas)

Oferta formativa de Foment Formació

Más información en el siguiente enlace

Legislación.

REGLAMENTO (UE) 2016/93 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 20 DE ENERO DE 2016 POR EL QUE SE DEROGAN DETERMINADOS ACTOS DEL ACERVO DE SCHENGEN (DOUE DE 2 DE FEBRERO DE 2016)

REGLAMENTO (UE) 2016/94 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 20 DE ENERO DE 2016 POR EL QUE SE DEROGAN DETERMINADOS ACTOS DEL ACERVO DE SCHENGEN EN EL ÁMBITO DE LA COOPERACIÓN POLICIAL Y JUDICIAL EN MATERIA PENAL (DOUE DE 2 DE FEBRERO DE 2016)

REGLAMENTO (UE) 2016/95 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 20 DE ENERO DE 2016 POR EL QUE SE DEROGAN DETERMINADOS ACTOS EN EL ÁMBITO DE LA COOPERACIÓN POLICIAL Y JUDICIAL EN MATERIA PENAL (DOUE DE 2 DE FEBRERO DE 2016)

Revistas

Seguritecnia Nº 427. Enero

Nuevo número de **SEGURITECNIA**, con reportajes, entrevistas y artículos, destacando:

- **Editorial:** Asuntos Pendientes *"ser lo que soy no es nada sin la seguridad"* (Shakespeare)
- **Seguripress**
- **Especial Prevención de Riesgos Laborales**
- **Entrevistas:** Gonzalo Castro, Presidente de la Asociación Catalana de Empresas de Seguridad (ACAES)

Enlace: ver revista digital

Cuadernos de Seguridad Nº 307. Enero.

En este número de **CUADERNOS DE SEGURIDAD**, además de las secciones habituales de «Seguridad», «Cuadernos de Seguridad estuvo allí», «Estudios y Análisis», o «Actualidad, el lector encontrará:

- **Editorial:** «Un año lleno de oportunidades».
- **En Portada:** «El sector ante 2016».
- **Artículos:** «Desafíos de la ciberseguridad en España».
- ***Un Café Con:*** «Ignacio Gibert, Jefe de Personal, Seguridad y Servicios de Cecabank».

Enlace: ver revista digital

red seguridad Nº 71. cuarto trimestre 2015.

Nuevo número de **RED SEGURIDAD**, con reportajes, entrevistas y artículos, destacando:

- Editorial bajo el título «Incertidumbre en el año nuevo».
- En Portada bajo el tema «Confianza. Nuevas metas».
- Corporativo: «Jornada sobre continuidad de negocio».
- Actualidad: «9ENISE. Escaparate global de la ciberseguridad».

Enlace: ver revista digital

¿Quieres ser Socio de ADSI – Asociación de Directivos de Seguridad Integral?

Para iniciar el proceso de alta como Asociado, envíe un e-mail a secretario@adsi.pro , indicando nombre y apellidos, una dirección de correo y un teléfono de contacto.

En cuanto recibamos su solicitud le enviaremos el formulario de Solicitud de Admisión.

¿Quién puede ser socio de ADSI – Asociación de Directivos de Seguridad Integral?

Puede ser socio de **ADSI**:

- Quien esté en posesión de la titulación profesional de Seguridad Privada reconocida por el Ministerio del Interior (T.I.P. de Director de Seguridad, Jefe de Seguridad, Detective Privado o Acreditación de Profesor de Seguridad Privada).
- Todo Directivo de Seguridad que posea, a criterio de la Junta Directiva de la Asociación, una reconocida y meritoria trayectoria dentro del sector.

www.adsi.pro

Asociación de DIRECTIVOS de SEGURIDAD Integral