Asociación Española de empresas de Seguridad

Dinamizando la Industria de la Seguridad

Boletín Informativo

Número 61 - Abril 2017

Carta del Presidente

Estimados asociados,

Finalizado ya el 1er trimestre de 2017, mediante esta cuarta carta me gustaría ponerte al corriente del trabajo de la Junta Directiva en este período.

Como os informamos, hemos comenzado con la presentación personal de nuestro "Manifiesto 2016 a 2019 por una España y una Europa más seguras y protegidas". El documento, que fue presentado oficialmente a los asociados en la Asamblea de AES celebrada el pasado 29 de noviembre, espera contribuir a desarrollar el enorme potencial de nuestra industria, con el que contribuir al crecimiento económico y al empleo sostenible. En este caso, queríamos empezar por las Fuerzas y Cuerpos de Seguridad, y tener reuniones con sus miembros, antes del 27 de abril, fecha en la que tendrá lugar el XII encuentro Seguridad Pública - Privada.

Así, las reuniones que han tenido lugar son las siguientes:

- El 1 de febrero, la Directora Ejecutiva y yo mismo, estuvimos en la Unidad Central de Seguridad Privada, con su jefe, el Comisario Principal D. Esteban Gándara.
- El 13 de febrero, la Directora Ejecutiva e Iñigo Ugalde, vocal de nuestra Junta Directiva, estuvieron en Erandio, en la sede de la Ertzaintza, con el Jefe de Seguridad Privada, D. Francisco Llaneza y otros miembros de la unidad.
- El 27 de febrero la reunión tuvo lugar con D. Andrés Sanz, Coronel Jefe del Seprose, y D. José Antonio Montero, Teniente Coronel del Seprose, y asistimos a la misma Paloma Velasco y yo en nombre de AES.
- El 2 de marzo nos desplazamos hasta Sabadell, a la sede de los Mossos, y posteriormente a la Dirección de Seguridad de la Generalitat, donde Anna Medina, Paloma Velasco, Antonio Escamilla y yo mismo presentamos nuestro manifiesto a miembros de la Unidad Central de Seguridad Privada de Mossos y a la Subdirectora de Seguridad de la Generalitat, Dª Maite Casado.
- Finalmente, el 21 de marzo, Javier Ruiz, vocal de nuestra Junta Directiva, y Paloma Velasco, tuvieron una reunión con el Coronel Jefe del ICAE, D. Domingo de Guzmán Caballero, y con el Capitán D. Manuel Luna.
- La reunión con el CNPIC, concretamente con José Ignacio Carabias, jefe de operaciones, y Juan José Zurdo, jefe del servicio de normativa y coordinación, tuvo lugar el 6 de abril.

Boletín Informativo de AES
Revista Trimestral - Abril 2017 - núm. 61

Edita:
Asociación Española de Empresas de Seguridad
C/Alcalá, 99 2ºA - 28009 Madrid
Telf. 915 765 225 - Fax 915 766 094
www.aesseguridad.es - aes@aesseguridad.es

Consejo de Redacción:
Antonio Escamilla Recio
Antonio Pérez Turró
Javier Ruiz Gil
Julio Pérez Carreño
Manuel Porras Borrajo
Manuel Sánchez Gómez-Merelo
Eduardo Mata Lorenzo
Óscar Tellez Carbajo

Coordina:
Paloma Velasco Merino

Diseño, Maquetación y Realización:
ERRE comunicación
www.erre-comunicacion.es

Terminada esta fase de presentaciones, se comenzará a presentar al Congreso, al Senado, al Ministerio del Interior, de Industria y de Defensa, y a los grupos parlamentarios del Congreso, reuniones que esperamos tengan lugar en el trimestre del año en el que ya nos encontramos.

Por otra parte, y continuando con el seguimiento de las áreas de trabajo de la Asociación (normalización y certificación, ingeniería, instalación y mantenimiento, seguridad electrónica, centrales receptoras de alarmas y seguridad física), las de seguridad electrónica y centrales receptoras de alarma han tenido ya dos reuniones en estos últimos tres meses. La de centrales receptoras de alarma concretamente, ha finalizado ya un documento de aportaciones para el borrador del Reglamento. La de seguridad física, está en la actualidad estudiando la creación de una subárea, de puertas de seguridad, en la que esperamos incluir próximamente a nuevos asociados de AES. El área de seguridad electrónica, ha emitido una nota de prensa juntamente con AEINSE, la Asociación Española de Ingenieros de Seguridad, sobre la formación de ingenieros de seguridad. También se ha hecho una propuesta para el borrador del Reglamento en esta materia.

> ***Se ha empezado a trabajar en la creación de una subárea de trabajo de ciberseguridad, que se encuadrará dentro del área de centrales receptoras de alarma.***

Además, se ha empezado a trabajar en la creación de una subárea de trabajo de ciberseguridad, que, de momento, se encuadrará dentro del área de centrales receptoras de alarma. Desde aquí te invito a que envíes un correo electrónico en el caso de que quieras participar en esta subárea de nueva creación. El objetivo de la misma es informar a nuestros asociados sobre todo el tema de las ciberamenazas, normativa, protección de datos, con espíritu pedagógico, así como crear un foro de consultas en esta materia para, con todo ello, impulsar dentro de las empresas interesadas, el desarrollo del negocio en esta emergente área de la seguridad.

Sobre el documento de recomendaciones para el diseño del sistema de seguridad física y electrónica a incluir en los planes de protección específicos de I.C., excelente trabajo conjunto de las áreas de seguridad electrónica y de ingeniería, instalación y mantenimiento y que fue presentado también en la Asamblea de noviembre, se hará una presentación en el XII encuentro de Seguridad Pública y Privada el próximo día 27 de abril.

Por último también comentarte que en este primer trimestre se ha publicado un Boletín Informativo en enero, y dos Newsletters en febrero y marzo. Ya sabes que puedes colaborar en nuestras publicaciones mediante artículos técnicos o de interés de la industria, siempre que no contengan publicidad.

Reiterarte finalmente mi disposición y la del resto de la Junta Directiva para cualquier comentario, sugerencia o aportación que quieras hacer para que AES siga "dinamizando la industria de la seguridad privada".

Saludos cordiales,
Antonio Pérez Turró
Presidente de AES.

Recuerdos e Historias

Antonio Ávila Chuliá

Los recuerdos tienen más poesía que
las esperanzas, como las ruinas
son mucho más poéticas que los planos
de un edificio en proyecto.

Una cosa es continuar la historia
y otra repetirla.

******

JACINTO BENAVENTE

Con las manos enfundadas en los bolsillos, la cabeza cubierta con gorra, abrigado, me dispongo a deambular por la Valencia de mis amores en este mes de marzo, a caballo entre el final del invierno y el comienzo de la primavera; con un clima inesperado en estas tierras levantinas, frío, pasado por agua, aunque predicho por los meteorólogos, hemos aguantado sucesivos frentes atlánticos que no van a impedir mi acostumbrado paseo, ni siquiera la "crida" de hace unos días, ¡ya estamos en Fallas!

Mientras camino observo el bullir de las gentes, el crecimiento del carril bici por doquier, organizador de tapones y algún atropello, por si eso no bastase proliferan los cortes de las vías públicas, el cierre de calzadas, típico en estas fechas, obras dondequiera que vayas, "mascletás"…; ando sin rumbo fijo, llego a la calle Juan Llorens, un gran andamio ocupa la acera, ello me hace elevar la mirada para fijarla en su frontis, se trata del Colegio Público Teodoro Llorente, titularidad de la Generalitat Valenciana, en cuya fachada unos albañiles se afanan en enlucir el agujero dejado al arrancar el escudo del Águila de San Juan; por si alguien lo ignora, esa heráldica es la misma que figura en la Constitución española de 1978, incluso presidió los debates de redacción y su promulgación hasta 1981, en que se sustituye por la actual divisa, más por ignorancia histórica que necesidad real.

Resulta curioso, con la de veces que he pasado por esa calle, nunca me diese cuenta que allí estaba el escudo de España con el Águila de San Juan, aguantando el paso de los años, sin molestar, cobijada en el exterior del frontispicio del colegio con apariencia neoclásica. Ahora quienes nos gobiernan, elegidos en democracia para cambiar a mejor la vida urbana y disfrutar de una ciudad más atrayente, agradable, fraterna, se dedican a destruir cualquier signo del pasado; de igual forma les afecta a los siervos de Dios como reparación de sus silenciados "pecados", para ello no se les ha ocurrido nada mejor que eliminar emblemas, distintivos, efigies, retratos y reescribir la historia, una verdadera torpeza, los hechos son tozudos, los históricos también, sin historia no se aprende de los errores del pasado, enseñanza que evita no tener que repetirlos en el presente y estropear nuestro futuro.

Me molestan estas ocurrencias, al tiempo, mi sesera no para de pensar mil cosas, así, sin venir a cuento, recuerdo al amigo Augusto, vecino de Roma, con quien en mis visitas de trabajo solía pasear por la tranquila y céntrica Vía Appia o Regina viarum, parque nacional, la más significativa y añeja de las calzadas de enlace construidas por los romanos. Evoco aquellas grandes caminatas rodeados de más de dos mil años de historia, igualmente alguna de nuestras conversaciones sobre todo su insistencia en un vetusto dicho romano: "Damnatio memoriae" (condena de la memoria), de uso habitual en la antigua Roma para castigar al enemigo después de su muerte. Hacían desaparecer cuanto pudiese evocar, revivir al condenado, de tal manera que suprimían y borraban el nombre del reprobado en imágenes, inscripciones e incluso se impedía usar su nombre. Quizás, pensaban que de esta forma desaparecería su historia, su vida, gran error, si algo se guarda para siempre es el pasado, bueno o malo.

Como añoso empresario, siempre me ha gustado de cuando en cuando mirar hacia atrás, comprobar el sendero transitado, el avance efectuado tras una larga existencia de esforzado trabajo. Esta práctica permite reconstruir fragmentos de la vida, analizar itinerarios peliagudos, angustiosos o alegres, con ilusiones cumplidas otras frustradas a mitad de trayecto, conocidas nuestras andanzas de este modo toman una visión singular al fin, camino recorrido en el pasado ejemplo de futuro.

Todos los padres tenemos en común el pretender lo mejor para nuestros hijos, queremos que destaquen en mil actividades, sean los más guapos, inteligentes, ricos, por desgracia no están solos en este mundo, la malicia, dureza, deslealtad, ingratitud, impera en demasía, es gratuita, individual o ejercida en grupo, poco importa, unos tratan de ocultarla, otros por el contrario la pregonan a los cuatro vientos, dan la cara, solo sirve para conocerlos, sea como fuere los jóvenes se la van a encontrar a lo largo de la vida. Creo, debemos darles una base sólida de autoestima, confianza en sí mismos, enseñarles a analizar los problemas y sus posibles soluciones, ayudarlos a descubrir sus habilidades para protegerse, en la historia y en los recuerdos familiares pueden encontrar parte de esa ayuda.

I Congreso de Ingeniería de Seguridad

El 22 de marzo se celebró el I Congreso de Ingeniería de Seguridad, una visión de la tecnología actual aplicada a la seguridad, organizada por Seguritecnia y AEINSE, a la que AES fue invitada.

De hecho, tanto nuestro presidente, Antonio Pérez, como Javier Ruiz, vocal de nuestra Junta Directiva, tuvieron sendas intervenciones, el primero sobre la protección antibalas y anti explosión y el segundo sobre normativa europea de seguridad. Antonio Pérez recalcó el hecho de que nuestra industria se dedica a "proteger personas". Por su parte, Javier Ruiz hizo un repaso por la historia y la evolución de UNE, anteriormente AENOR, asegurando que la seguridad "tiene que ser integral".

Otras intervenciones fueron la de Óscar Sacristán, que habló de las necesidades de monitorización de sistemas y usuarios en Seguridad CCTV, Gerardo Estalrich, de Bosch Security Systems, empresa asociada en AES que expuso una serie de consideraciones de seguridad de datos y nuevas normativas europeas de seguridad y protección en el diseño de un proyecto de seguridad, invitando a la reflexión ya que hay un incremento notable del número de cámaras instaladas. ¿Cómo manejamos esa cantidad de datos? ¿Dónde los vamos a almacenar? Y estableciendo una serie de pasos fundamentales:

1) Crear confianza
2) Asegurar los datos.
3) Establecer el derecho de acceso.
4) Cumplir con los estándares de la industria.

Por otro lado intervinieron Enrique Bilbao (la convergencia de la seguridad, análisis de los riesgos físicos y lógicos), Javier Castillo (de la monitorización a los sistemas PSIM), Joaquín Castillejo (el reto de la inteligencia en la industria), José Ignacio Álvarez (plataforma de integración abierta para sistemas de seguridad), David Soto (alta tecnología para la supervisión de vehículos en los entornos más críticos) y Roberto Montejo y Enrique Esteban (visión térmica para la protección perimetral).

En la Mesa Redonda sobre certificación y formación de ingenieros de seguridad, Manuel Yanguas, Comisario de la Unidad Central de Seguridad Privada, explicó que la Ley distingue entre personal de seguridad privada y personal acreditado, dentro del cual se comprenderían los profesores, los ingenieros, los técnicos y los operadores de seguridad, y que la ley prevé que estos profesionales sean acreditados por su honorabilidad y con presentación de sus antecedentes penales.

Pedro Carpintero, presidente de AEINSE, en su intervención, pidió que, además, tuvieran una formación académica.

En este sentido nos remitimos a la nota de prensa que AES ha emitido conjuntamente con AEINSE y que se ha publicado en el número de marzo de Seguritecnia, aquí.

La Necesaria y Pendiente Calificación UNE 62676

por Julio Pérez Carreño,
Secretario de la Junta Directiva de AES.

Tal y como establece la Orden Ministerial INT/316/2011 en su artículo 3, relativo a la aprobación de material de seguridad privada para ser comercializado y ser utilizado en los servicios de seguridad privada, *"cualquier elemento o dispositivo que forme parte de un sistema de alarma de los recogidos por la normativa de seguridad privada, deberá cumplir, como mínimo, el grado y características establecidas en las Normas UNE-EN 50130, 50131, 50132, 50133, 50136 y en la Norma UNE CLC/TS 50398, o en aquellas otras llamadas a reemplazar a las citadas Normas, aplicables en cada caso y que estén en vigor"*.

Cuando nos referimos a sistemas de alarma contra intrusión la familia UNE–EN 50131-X, recoge por un lado los distintos detectores de interior, como los de infrarrojos pasivos (UNE–EN 50131-2-2), los detectores de microondas (UNE–EN 50131-2-3), los detectores combinados de infrarrojos pasivos y microondas (UNE–EN 50131-2-4), los detectores combinados de infrarrojos pasivos y ultrasónicos (UNE–EN 50131-2-5), los contactos magnéticos (UNE–EN 50131-2-6) y los detectores de rotura de cristal (UNE–EN 50131-2-7), y por otro lado recoge las centrales de alarma y señalización (UNE–EN 50131-3), los dispositivos de advertencia (UNE–EN 50131-4) y las fuentes de alimentación (UNE–EN 50131 -6).

De esta manera podemos configurar una instalación de sistemas de detección de intrusión en interiores, utilizando elementos normalizados y por lo tanto potencialmente certificables, en la gran mayoría de los casos, con la significativa excepción de los detectores sísmicos cuya norma correspondiente continúa en fase de elaboración a día de hoy. Sin embargo cuando lo que se pretende es la protección en exteriores (sistemas perimetrales) la ausencia de normas para la selección de elementos es absoluta, disponiendo solo en estos casos de la norma (CLC/TS 50131-7), que no obstante constituye una valiosa guía de aplicación para la instalación de sistemas de intrusión, tanto en interiores como en exteriores, con el menor número de alarmas indeseadas posibles. Para ello proporciona consejos relativos al diseño, a la instalación, al mantenimiento e incluso a la operación de dichos sistemas.

La CLC/TS 50131-7, no es por lo tanto una Norma que posibilite la normalización y posterior certificación de los distintos elementos a utilizar, sino una guía o especificación técnica que pretende garantizar la existencia de sistemas de detección de intrusión fiables y eficaces.

De acuerdo a la UNE-EN 50131-1 los sistemas de detección contra intrusión podrán adoptar distintos grados de seguridad en función de la esperada cualificación de los posibles intrusos. Según la clasificación establecida el grado de seguridad más bajo (grado 1) supondría que los intrusos poseerían muy escasos conocimientos de los sistemas instalados y que en su ataque solo utilizarían por tanto unas limitadas herramientas de fácil adquisición. Por el contrario el grado de seguridad más alto (grado 4), estaría previsto para usar en los casos en los que fuera previsible el ataque por intrusos con conocimientos, habilidades y recursos suficientes para evadir e incluso sabotear los distintos componentes del sistema de intrusión.

Paralelamente desde la citada Orden Ministerial INT/316/2011, en su artículo 2, se incorporan dos nuevos criterios en la graduación de la seguridad de los sistemas, incluyendo por un lado la naturaleza y características del lugar a proteger y por otro la obligatoriedad o no, de conectar dichos sistemas con una central receptora de alarmas o con un centro de control. Se establecen por tanto otros cuatro grados de seguridad que se hacen corresponder con los existentes en la UNE-EN 50131-1, de manera que:

El grado 1 de la citada norma se corresponde con los sistemas de Grado 1, o bajo riesgo, que serán sistemas que no se van a conectar a una central receptora de alarmas o a un centro de control.

Los de Grado 2, de riesgo bajo a medio, serán dedicados 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.

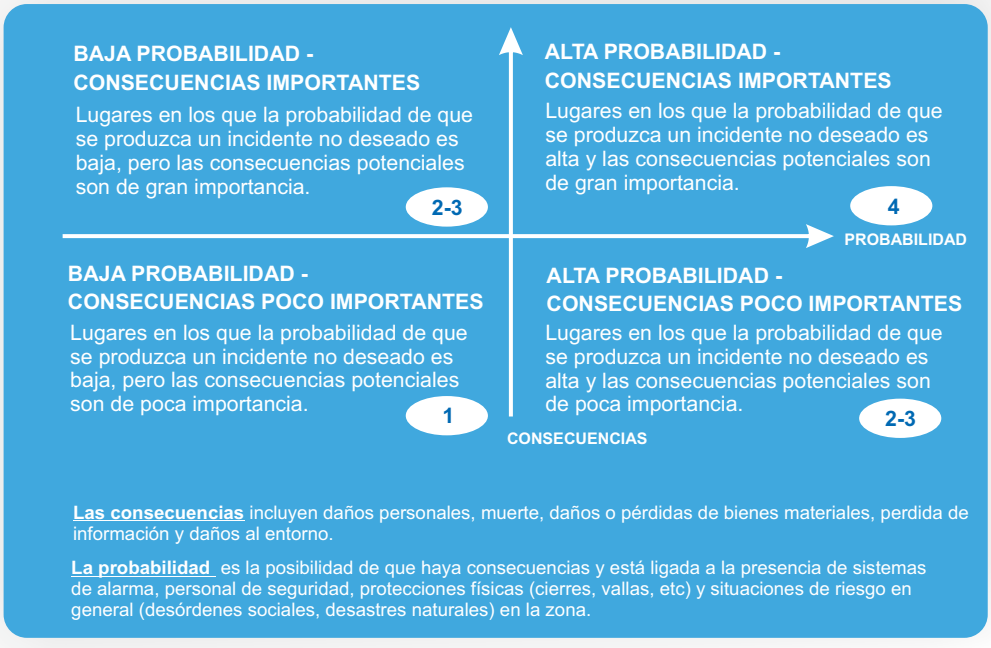
Los de Grado 3, de riesgo medio/alto, destinados a establecimientos obligados a disponer de medidas de seguridad, de acuerdo a lo establecido por el Real Decreto 2364/1994 ó al reglamento de próxima aparición de la vigente Ley 5/2014, así como a otras instalaciones comerciales o industriales a las que 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.

Por último los de 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.

Los cuatro grados establecidos tanto en la UNE-EN 50131-1 como en la Orden Ministerial INT/316/2011, podrán correlacionarse de manera biunívoca, de manera que el grado establecido en una de ellas pueda ser adoptado por la otra.

Desde el pasado mes de Diciembre, la norma EN 50132-1:2010, referente a los Sistemas de Vigilancia CCTV para uso en aplicaciones de seguridad, ha sido sustituida y actualizada por la UNE-EN 62676-1-1:2015 aunque no será de obligado seguimiento hasta dentro de treinta meses. (Junio de 2019)

La nueva norma UNE-EN 62676-1-1: 2015 empieza por renombrar, acertadamente, los hasta ahora denominados Circuitos Cerrados de Televisión (CCTV) por Sistemas de Videovigilancia (VSS, por sus siglas en inglés, *Video Surveillance Systems*) y recoge los requisitos mínimos que debe cumplir un sistema (VSS) que vaya a formar parte de un sistema de seguridad conectado a una Central Receptora de Alarmas (CRA) o a un centro de control. Debemos entender por tanto que esta nueva norma, tiene una directa relación con la Seguridad, y que por ello debe tener una lógica consecuencia en su incorporación a la legislación de seguridad privada.



Al igual que ocurre en el diseño de un sistema de detección de intrusión, los resultados de la necesaria evaluación del riesgo deben utilizarse para determinar los requisitos del Sistema de Videovigilancia (VSS) y de sus distintos componentes y por ende el grado de seguridad a adoptar por el VSS. Los grados establecidos para el VSS en la norma UNE-EN 62676-1-1:2015 se han configurado teniendo en cuenta el nivel de riesgo dependiente de la probabilidad de que se produzca un incidente y del daño potencial causado por él, como se muestra en la figura anexa extraída de la citada Norma.

Al confrontar los niveles de riesgo establecidos en la Orden Ministerial INT/316/2011, la UNE-EN 50131-1 y la nueva UNE EN 62676-1-1:2015, nos encontramos con un importante escollo dado que los criterios no son exactamente intercambiables ni biunívocos.

Es necesario por tanto convenir la correlación de todos ellos de manera que:

CRITERIO	NIVEL 1	NIVEL 2	NIVEL 3	NIVEL 4
OM INT/316/2011	Bajo riesgo, no conectables a una central receptora de alarmas o a un centro de control.	Riesgo bajo a medio, serán dedicados a viviendas y pequeños establecimientos, comercios e industrias en general, conectados a una central de alarmas o a un centro de control.	Riesgo medio/alto, destinado a establecimientos obligados a disponer de medidas de seguridad u 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 a un centro de control.	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,
UNE EN 50131-1	Bajo riesgo: Intrusos con conocimientos muy escasos de los sistemas de seguridad y con herramientas muy limitadas.	Riesgo bajo a medio: Intrusos con conocimientos limitados de los sistemas de seguridad y con herramientas generales e instrumentos portátiles.	Riesgo Medio a Alto: Intrusos con conocimientos de los sistemas de seguridad y con herramientas y equipos electrónicos portátiles.	Riesgo Alto: La seguridad es prioritaria sobre todos los factores. Los intrusos conocen los sistemas y disponen de recursos para planificar la intrusión con una gama completa de equipamiento para evadir o incluso sabotear los sistemas.
UEN EN 62676-1	Baja Probabilidad y Consecuencias poco importantes.	Alta Probabilidad y Consecuencias Poco Importantes.	Baja Probabilidad y Consecuencias importantes.	Alta probabilidad y Consecuencias importantes.

Sin embargo y a diferencia de la familia UNE–EN 50131-X, la UNE EN 62676-1, establece ya en su introducción que no tiene como objetivo su utilización para someter a ensayo a los componentes individuales de un VSS. No podremos esperar por tanto de ella la normalización de los distintos componentes ni como consecuencia, su posible certificación.

Tal y como expone la Norma podemos definir un sistema de Videovigilancia (VSS) como un conjunto de partes funcionales y las relaciones que existen entre ellas. Un Vss utilizado en aplicaciones de seguridad se puede presentar en bloques funcionales que describen las distintas partes y funciones del sistema según la figura anexa extraída de la citada Norma.

El diseño de un adecuado VSS no dependerá tanto de la utilización de un equipamiento concreto con unas características determinadas sino de la funcionalidad que proporciona al sistema de seguridad para el que está concebido. Estas funcionalidades no son intrínsecas a un componente del sistema ni siquiera a uno de los tres entornos expuestos (Entorno de Vídeo, Gestión del Sistema y Seguridad del Sistema), incluso un único dispositivo podrá realizar varias funciones. Una cámara de televisión podrá, por ejemplo, capturar las imágenes, almacenarlas temporalmente, analizarlas y procesarlas e incluso transmitirlas para su envío a través de la red.

Consecuencia de todo ello y de la imposibilidad de normalizar el distinto equipamiento para su instalación con determinado grado de seguridad, lo que la norma 62676 en su parte 4 expone, son directrices de aplicación y establece una lista de diez y ocho funcionalidades, que conformarán los criterios a tener en cuenta para definir el grado de seguridad de un VSS.

La funcionalidades establecidas son: las Interconexiones comunes, la capacidad de Almacenamiento, el Archivado y copia de seguridad, La Información relacionada con la alarma, los Registros del sistema, la Copia de seguridad y la restauración de los datos del sistema, la Notificación de fallo repetitivo, la protección contra la manipulación de imágenes, el Tiempo de espera del búfer de imagen, las Funciones esenciales de fallo de un dispositivo y el tiempo de notificación, el Monitoreo de interconexiones, la Detección de manipulaciones, los Requisitos de código de autorización, la Sincronización de tiempos, la Autenticación de datos, la Autenticación de exportación / copia, el Etiquetado de datos y la Protección de datos (manipulación)

La norma UNE-EN 62676-1-1:2015 proporciona un nuevo enfoque global para los sistemas de video vigilancia en contrapunto a las tradicionales normas de producto, definiendo el uso de “buenas practicas” y un conjunto de instrucciones con las que garantizar:

- que las necesidades de un usuario potencial estén debidamente especificadas y entendidas.
- que el sistema esté diseñado, instalado, operado y mantenido para satisfacer las necesidades del usuario:
  - Permitiendo la comparación entre las propuestas de los proveedores.
  - Permitiendo la aplicación coherente de las funciones.
  - Proporcionando un método simplificado para especificar un sistema.

De esta manera las distintas funcionalidades descritas podrán ser exigibles o no, en mayor o menor medida, en función del grado de seguridad que se haya asignado al sistema, pudiendo incluso disponer de un sistema con un grado de seguridad superior en alguna de las funcionalidades o incluso inferior si aquella funcionalidad en concreto no fuera precisa.

Podremos tener recomendaciones de grado para cada una de las funcionalidades, y el grado de la instalación será aportado por el diseñador de la instalación en primer término y del instalador posteriormente. El requisito de que un elemento o componente individual sea capaz de satisfacer una funcionalidad especificada en la norma no es fácil, dado que cómo hemos expuesto esta funcionalidad podrá ser aportada por varios de los elementos elegidos en cualquiera de los tres entornos definidos o incluso suponiendo que un elemento pudiera

aportar los requerimientos para posibilitar una funcionalidad en un grado determinado, este dependerá del sistema en el que vaya instalado.

Existirán no obstante ciertos requerimientos relevantes que un producto no será capaz de cumplir en un grado superior, esta circunstancia sí limitará claramente ese producto concreto sin importar lo que el resto del sistema aporte.

Debemos entender por tanto que a pesar de la regulación establecida por la OM INT 316/2011 para la adopción y certificación del grado de seguridad en los sistemas de Videovigilancia (VSS), la normalización aportada por la UNE –EN 62676 no posibilita la certificación de componentes o productos individuales, sino la regularización de determinadas funcionalidades y su grado de cumplimiento en función de los niveles de seguridad en ella establecidos.

De esta misma opinión es la British Security Industry Associations (BSIA) según se desprende del análisis de los documentos publicados en su web. Form 217 – BS-EN 62676 series – Guidance for customers about grading and other important matters and Form 218 – Grade requeriments under BS EN 62676 standard for CCTV)

En este contexto surge la necesidad de concretar, cómo y quién debe certificar una instalación de Videovigilancia y el papel que en ello deben representar las figuras de Técnico e Ingeniero indicadas en la Ley 5/2014 como personal Acreditado según se expone en su artículo 19.1.c y en el artículo 46.1, y salvando lo indicado en el artículo 52.2.

La controversia está servida.

Reuniones presentación del Manifiesto AES

Durante este mes, han tenido lugar dos reuniones más, en el ICAE y en el CNPIC.

El día 21 de marzo, Javier Ruiz y Paloma Velasco tuvieron una fructífera reunión de presentación con el capitán Manuel Luna, del ICAE, y el Coronel Domingo de Guzmán Caballero. En ella los miembros del ICAE elogiaron la iniciativa de AES, e invitaron a presentar el Manifiesto en instituciones como el Ministerio de Defensa.

Por otro lado, el día 6 de abril, representantes de la Junta Directiva, en concreto el Presidente y el Vicepresidente, y la Directora Ejecutiva, se acercaron a El Pardo, y mantuvieron una reunión de presentación con el CNPIC. José Ignacio Carabias y Juan José Zurdo fueron los representantes del Centro que escucharon la intención de nuestro Manifiesto y se pusieron a disposición de nuestros asociados para todo lo relativo a la protección de Infraestructuras Críticas.

¿Es legal tratar datos biométricos con el Reglamento Europeo de Protección de Datos?

La pregunta surge al hilo de la nueva regulación establecida por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, también llamado, el Reglamento General de Protección de Datos (en adelante RGPD) que ha clasificado a los datos biométricos como "categorías especiales de datos".

La razón de ello: el hecho de que este tipo de datos permiten la identificación o la autenticación unívocas de una persona física. Es un cambio normativo importante, frente a la actual regulación que, aunque no prohíbe el tratamiento de este tipo de datos, los biométricos, sí los somete a condiciones y garantías específicas. Esto afectará a un gran número de responsables de ficheros que, fundamentalmente, llevan a cabo la recogida de datos biométricos en el ámbito de los recursos humanos para la gestión de control de acceso, control horario y control presencia.

Quizás la primera pregunta sería entender la definición que de "dato biométrico" tiene el RGPD. En este punto, el RGPD define a los «datos biométricos» como aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

En relación con las imágenes faciales, el RGPD en todo caso especifica que, el tratamiento de fotografías no debe considerarse sistemáticamente un "tratamiento de categorías especiales de datos personales", quedando únicamente comprendidos en este caso como datos biométricos aquellas imágenes fotográficas faciales tratadas con medios técnicos específicos que permitan la identificación o la autenticación unívocas de una persona física.

Y qué consecuencias prácticas tiene la nueva categorización de los datos biométricos como "categorías especiales de datos". Según se indica en el RGPD, varias son las consecuencias a tener en cuenta:

En primer lugar, tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el Reglamento o en Derecho de los Estados miembros.

En este sentido, según el RGPD, los Estados miembros deben autorizar las excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular por ejemplo, el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad.

En esta línea, el propio RGPD prohíbe el tratamiento de datos personales biométricos salvo que el tratamiento sea necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, pero únicamente en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo que establezcan garantías adecuadas del respeto de los

derechos fundamentales y de los intereses del interesado;

En segundo lugar, además de los requisitos específicos para este tipo de tratamientos, deben aplicarse los principios generales y otras normas contenidas en el RGPD, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. En este sentido, además, el RGPD faculta a los Estados miembros para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos biométricos.

Entre estas medidas o condiciones específicas para el tratamiento de datos biométricos, debemos destacar las siguientes:

La realización de una evaluación de impacto relativa a la protección de datos con apoyo y asesoramiento del delegado de protección de datos, cuando haya sido nombrado. La evaluación deberá incluir como mínimo: a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento; b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; c) una evaluación de los riesgos para los derechos y libertades de los interesados d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Para esta evaluación de impacto se tendrá en cuenta las repercusiones de las operaciones de tratamiento realizadas por el responsable o encargados, y además, cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes.

Realizada la evaluación de impacto, el responsable del tratamiento deberá consultar a la autoridad de control (Agencia Española de Protección de Datos) antes de proceder al tratamiento cuando la evaluación de impacto muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo. Y en estos casos, la autoridad de control deberá asesorar por escrito al responsable, y en su caso al encargado.

Otra medida específica será la de llevar a cabo un registro de las actividades de tratamiento efectuadas bajo su responsabilidad, que contenga al menos: a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos; b) los fines del tratamiento; c) una descripción de las categorías de interesados y de las categorías de datos personales; d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales; e)en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, cuando corresponda, la documentación de garantías adecuadas; f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos; g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

En caso en que el responsable haya contratado los servicios de un encargado del tratamiento, también será preciso que el encargado lleve un registro de actividad con una información similar a la expuesta (aunque con algunas diferencias).

Finalmente, tanto el responsable como el encargado de tratamiento con datos biométricos, deberán nombrar un delegado de protección de datos, que tendrá, entre otras, las siguientes funciones mínimas: a) informar y asesorar al responsable o al encargado del tratamiento y a los

empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos; b) supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes; c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación; d) cooperar con la autoridad de control; e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, y realizar consultas, en su caso, sobre cualquier otro asunto.

En todo caso es importante tener en cuenta que, las medidas descritas, no son las únicas que se deberán tener en cuenta a la hora de adoptar las garantías exigidas por la normativa sobre protección de datos para tratar datos biométricos. Además de lo anterior, el responsable deberá garantizar los derechos de los individuos además de los principios de transparencia, legitimidad, confidencialidad y seguridad.

Respondiendo a la pregunta inicial, el tratamiento de datos biométricos no quedará prohibido por el RGPD, pero sí sujeto a unas garantías específicas y robustas que afectarán, tanto a las empresas que utilicen sistemas biométricos para la gestión laboral o de la seguridad, como para las empresas de seguridad (o proveedores de tecnología) que se ocupen del mantenimiento de los sistemas de recogida y almacenamiento de dichos datos.

Ana Marzo
EQUIPO MARZO

Agenda Ferias 2017

- ISC WEST, 5 – 7 abril. Las Vegas.
- WORLD METRO RAIL CONGRESS, 25 y 26 de abril. Londres.
- SECURITY & COUNTER TERROR EXPO, 3 – 4 mayo. Londres.
- SECURITY FORUM, 17 – 18 mayo. Barcelona.
- FERROFORMA, 6 – 8 junio. Bilbao.
- CYBER GUARD - The European Cyber Security Summit – 15 – 16 junio. Praga
- III CONGRESO EDIFICIOS INTELIGENTES, 20 – 21 junio. Madrid.
- IFSEC, 20 – 22 junio. Londres.
- KAZBUILD, 5 – 8 septiembre. Kazajistán.
- SECURTEC CUBA, 19 – 21 septiembre. La Habana.
- SECURITY USER EXPO, 27 – 28 septiembre. Copenhague.
- ICCST-2017: 51st International Carnahan Conference on Security Technology, 23 – 26 octubre. Madrid.
- SMART CITIES EXPO WORLD CONGRES, 14 – 16 noviembre. Barcelona.
- SICUREZZA, 15 – 17 noviembre. Milán.
- MILIPOL, 21 – 24 noviembre. París.

Jornada sobre la Excelencia en la Contratación Pública

AES invitada a la jornada sobre Excelencia en la Contratación Pública, organizada por APROSER y Forética, tuvo lugar el pasado 24 de marzo en la sede de la CEOE, la jornada sobre excelencia en la Contratación Pública.

Dicha jornada, fue abierta por el presidente de Aproser, Ángel Córdoba, el cual recalcó el retraso en la trasposición de la Directiva Europea al ordenamiento jurídico español.

Aproser ha encargado un estudio a Forética sobre la contratación pública, en el que se muestran las luces y las sombras. El primer muro que se ha puesto de manifiesto es las medidas que se llevaron a

cabo contra la crisis, la prevalencia de lo cuantitativo sobre la calidad.

El segundo muro, la reforma laboral, que no tiene en cuenta la peculiaridad de los sectores intensivos en mano de obra.

Seguidamente intervino Jaime Silos, de Forética, que realizó una presentación del estudio, con cinco puntos.

1) Compra pública responsable. Se destinan dos billones de euros, es decir, el 16% del PIB de Europa, por pate de los estados miembros, a la contratación pública. Los países más sostenibles suelen ser los más competitivos.
2) Servicios de seguridad privada, un sector idóneo para la contratación pública. Esta idea se basada en que hay un impacto positivo en el mercado de trabajo de la seguridad privada debido a factores como el dividendo social, las sinergias con la seguridad ciudadana, la autoridad responsable, el trabajo digno, el desarrollo profesional, las ciudades inteligentes, la reducción de la siniestralidad o las instalaciones críticas.
3) La situación del sector de la Seguridad Pirvada en responsabilidad social. Es un sector muy avanzado en la implantación de sistemas de gestión.
4) Retos y oportunidades.
   Dentro de los primeros están los siguientes:
   - Involucración de grupos de interés.
   - Presión sobre las condiciones laborales.
   - Marco legislativo no consolidado.

   Dentro de las oportunidades, se encuentran:
   - Responsabilidad social corporativa como ventaja competitiva.
   - Políticas de empleabilidad para colectivos de riesgo.
   - Mayor transparencia.
5) Conclusiones: hay que alinear el mandato de la Administración y el marco legal que dé soporte. El sector de la Seguridad Privada tiene prácticas consolidadas y la aplicación de la responsabilidad social hace que la Administración cuente con estas ventajas, además de la calidad, el precio y el servicio social.

Seguidamente hubo una mesa redonda coordinada por Eduardo Cobas, y en la que participaron Juan Manuel Salgado, del Patrimonio Nacional, presentado por Basilio Febles de USO, Jesús Alejandro Vidart, de la Comunidad de Madrid, presentado por Daniel Montoya, de CCOO y Begoña Fernández, del Ayuntamiento de Madrid, presentada por Diego Giráldez, de UGT, donde se habló de las buenas prácticas en la contratación pública.

Más información en:
http://foretica.org/rsc_en_contratacion_publica_servicios_seguridad_privada.pdf
https://cincopa.com/~A4HAN6NguHRM

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.