

## SEGURITECNIA

MÁS DE 300 PROFESIONALES AVALARON EL ÉXITO DE LA JORNADA SOBRE GESTIÓN DE ALARMAS



## Gestión de alarmas: grandes logros que exigen continuidad

Desde que el Ministerio del Interior aprobó una orden en 2011 para poner freno a las falsas alarmas que recibían las Fuerzas y Cuerpos de Seguridad, el panorama ha cambiado sustancialmente. Sin embargo, parece que el problema no está resuelto del todo, por lo que la comunicación entre las empresas que reciben las alarmas y las instituciones policiales es fundamental para continuar avanzando. Con ese objetivo, *Seguritecnia* organizó el 17 de septiembre, en Madrid, la jornada *Servicios de gestión de alarmas: Evolución tecnológica e impacto social*. Un evento que muy pocos se quisieron perder y que reunió a más de 300 profesionales de esta actividad. El aforo puso de manifiesto que, sin duda, este es uno de los asuntos que despiertan mayor atención para el sector de la seguridad privada.

Por B. Valadés, E. González y L. Borredá

Como no podía ser de otra manera, a tenor de su importancia y del interés que ha suscitado en el sector, la jornada *Servicios de Gestión y Control de Alarmas. Evolución Tecnológica e Impacto Social* organizada por *Seguritecnia*, con el apoyo de los patrocinadores Security Cloud Services, Securitas Direct, Tyco Security Products y Alai Secure, abordó la nueva Ley de Seguridad Privada en lo que a las centrales receptoras de alarmas (CRA) se refiere, y también se debatieron cuestiones que, a juicio de los ponentes, debería contemplar y definir el futuro texto reglamentario.

El encargado de detallar todo aquello fue Luis González Pernía, jefe del Grupo de Medidas e Instalaciones de la Unidad Central de Seguridad Privada (UCSP) del Cuerpo Nacional de Policía. Tras una breve introducción basada en el preámbulo de la Ley, el inspector jefe comenzó explicando que una de las novedades de la misma tiene que ver con “la monitorización de cual-

quier señal de dispositivos auxiliares para la seguridad de personas, bienes muebles o inmuebles o de cumplimiento de medidas impuestas. Lo que se ha hecho es introducir lo ya contemplado por la orden ministerial INT/316 de 2011 en un ámbito legal superior”, precisó.

González Pernía también se refirió a lo que era “un clamor” por parte del sector de la seguridad privada: las actividades compatibles –fuera del ámbito de aplicación de la nueva Ley–. Entre ellas, se encuentran “las conexiones a CRA de sistemas de alarmas de tipo técnico o asistencial o las relacionadas con servicios de control o mantenimiento”. Igualmente, destacó que, sean o no de seguridad privada, “a las empresas que se dediquen a las actividades de seguridad informática se les podrá imponer reglamentariamente requisitos específicos para garantizar la calidad de los servicios que presten”, cuestión abordada posteriormente en la mesa redonda destinada a hablar del futuro reglamento.

En su desglose de novedades, Luis



Luis González Pernía, Cuerpo Nacional de Policía.

González Pernía hizo alusión al personal acreditado: “profesores de centros de formación, ingenieros, técnicos y operadores de seguridad. Estos últimos deberán disponer de la correspondiente acreditación expedida por el Ministerio del Interior –no necesaria para los trabajadores que, a la entrada en vigor de la Ley, estuvieran desempeñando su actividad en una CRA–. Teniendo en cuenta que ahora se exige una acreditación profesional, sería conveniente

demandar algunos cursos de formación”, propuso el inspector jefe.

La ampliación de las funciones de los vigilantes de seguridad o el procedimiento sancionador –también comentado en la posterior mesa redonda– fueron otros de los temas tratados por González Pernía, quien puso especial énfasis en puntualizar que, en el caso de los servicios de verificación personal, las CRA deben subcontratar dicha prestación. De no ser así, “incurrirían en una falta muy grave”.

## Propuestas

Tras la intervención de González Pernía se celebró la mesa redonda *Ley de Seguridad Privada y futuro reglamento*, moderada por Ana Borredá, directora de *Seguritecnia*, y en la que tomaron parte Pedro de Ibarrondo, consejero delegado de Security Cloud Services; Ángel Vázquez, director de Ventas para el Sur de Europa de Tyco Security Products; Javier Anaya, director comercial de Alai Telecom; y José Ignacio Jiménez del Castillo, director de Relaciones Institucionales de Securitas Direct.

Antes de entrar en materia, Borredá anunció que esa misma mañana, junto a representantes de las principales asociaciones, había sido recibida por Francisco Martínez Vázquez, secretario de Estado de Seguridad, al que se hizo entrega de “un documento consensuado por una importante representatividad del sector de la seguridad privada” con propuestas para elaborar el futuro texto reglamentario.

Respecto a este último, preguntó a los ponentes si el concepto de CRA se había quedado obsoleto y debería quedar plasmado en el nuevo reglamento con otra terminología. El *guante* lo recogió Pedro de Ibarrondo, quien esclareció que “compañías como el BBVA denominan centro de gestión de alarmas a lo que durante tantos años se ha llamado CRA”. “Creo que esa es la tendencia a seguir y lo valoro positivamente, ya que contribuiría a aumentar el número de servicios que se puedan prestar y, por lo tanto, al crecimiento de las centrales”, añadió.



A continuación salió a la palestra un tema *caliente* para las CRA: las revisiones y el mantenimiento de los sistemas. Según Ángel Vázquez, “en la actualidad hay una especie de *tira y afloja* entre lo que se hace y lo que sería deseable. Y una discrepancia sobre quién tiene que llevar a cabo esas operaciones, cómo y cuántas veces”. “Bajo mi punto de vista, el número debe ser el mínimo para asegurar que todo funciona correctamente. En el caso del Grado 2 de seguridad –de riesgo bajo a medio y relativo a viviendas y pequeños establecimientos, comercios e industrias en general–, bastaría una revisión presencial y tres remotas. Por lo que respecta al Grado 3 –de obligado cumplimiento en establecimientos e instalaciones de riesgo medio/alto–, podría establecerse un protocolo similar, pero con la presencia del usuario en alguna de las revisiones remotas”, continuó.

## Comunicación segura

Las vías de comunicación –en concreto, si el reglamento puede contribuir a garantizar que sean más seguras– fue otro de los temas que se trató en la mesa redonda. Al respecto, Javier Anaya opinó que “sería necesario regularizar la *securización* de las líneas, *encriptarlas* de tal forma que sea imposible invadirlas. Recientemente, hemos visto que el servicio de almacenamiento de datos iCloud de Apple ha sido vulnerado y las consecuencias que ha tenido dicha acción: la filtración masiva de fotografías íntimas de personajes famosos. Si no garantizas la *securización*, al final controlarán no sólo tus imágenes, también tu casa o alarma”.

Llegados a este punto, Ana Borredá instó a los ponentes a considerar si el texto reglamentario tendría que contemplar una definición exacta y de fácil comprensión de lo que se entiende por doble vía de comunicación –red



de cable e inalámbrica, como precisó Ángel Vázquez-. Sobre esta cuestión, Javier Anaya manifestó que “efectivamente, el reglamento debería explicar qué es dicho concepto y en qué consiste. Y también hacer hincapié en que las dos vías de comunicación sean obligatorias en los grados 3 y 4” –este último, considerado de alto riesgo y reservado a las infraestructuras críticas, instalaciones militares, empresas encargadas de la custodia de efectivo, valores, metales preciosos...–.

En relación con este apunte de Anaya, Pedro de Ibarrodo coincidió con él, añadiendo que la doble vía de comunicación “podría ser recomendable para los sistemas de alarma englobados en el Grado 2”.

Además, el consejero delegado de Security Cloud Services puntualizó que, en el caso de sectores estratégicos o infraestructuras críticas, se deberían reforzar las acciones para protegerse de “ciberataques y tener a buen recaudo las bases de datos o la información sensible. Igualmente, conviene preguntarse qué sucedería si se caen las comunicaciones en los centros que se dedican a proteger ese tipo de instalaciones”. “Yo propongo que sea obligatorio algún tipo de certificado, de revisión anual, que asegure un plan de contingencia ante situaciones así”, añadió sobre esta cuestión.

## Verificación

Otro de los asuntos *candentes* de la mesa redonda fue el relativo a la verificación secuencial. Así, José Ignacio Jiménez del Castillo recordó: “la necesidad de que se produzca el salto de tres elementos en menos de 30 minutos para poder confirmar una alarma, y dar aviso a las Fuerzas y Cuerpos de Seguridad (FCS), se discutió en su momento. En el sector consideramos que era algo incongruente y la realidad nos lo ha acabado demostrando. En ocasiones, la espera a esos tres saltos ha retrasado la actuación policial o ha ocasionado que la misma no fuese avisada”.

“Con el salto de un elemento, las CRA ya tenemos que estar alerta para ave-



riguar qué está sucediendo en una vivienda o negocio. Y en el supuesto de que se produzcan dos –por ejemplo, en la entrada y el salón–, y no se pueda verificar de otra manera o localizar al usuario, no es lógico que la central no esté habilitada para dar aviso a los servicios policiales. Nuestro día a día nos dice que esos saltos están provocados por una intrusión. Este es un asunto que se debe valorar y ahora es el momento de actuar y corregir”, comentó el representante de Securitas Direct.

Al hilo de esta exposición, Pedro de Ibarrodo señaló que en Cataluña se puede avisar a los Mossos d’Esquadra “si se activan dos detectores de una instalación. Hay centrales que no han atendido alarmas reales por esperar al tercer salto. Si allí ha habido buenos resultados, tomemos ejemplo. De sabios es rectificar”.

Por su parte, Ángel Vázquez consideró interesante dotar a los detectores de los nuevos sistemas de “una tecnología que ayude a verificar mejor las alarmas”.

Continuando con las verificaciones, también se debatió sobre las realizadas presencialmente. Para José Ignacio Jiménez del Castillo: “la verificación personal tiene muchas posibilidades, pero, a día de hoy, es una prestación que, bajo mi punto de vista, está encorsetada. Enviar a un vigilante, con o sin llaves, a una instalación para comprobar qué está ocurriendo en ella es complejo y caro; y si además el profesional se encuentra con limitaciones, el servicio acaba siendo ineficaz”.

“En una verificación personal, la actuación del vigilante debería ser más abierta. Me sorprende, a tenor de la exposición de Luis González Pernía sobre la nueva Ley de Seguridad Privada, que no pueda verificar una alarma de fuego. Sí, estamos de acuerdo en que no está cualificado para hacer frente a un incendio ni tampoco para combatir el delito. De eso se encargan los bomberos y las FCS, respectivamente. Pero si alguien contrata un servicio de acuda, ¿qué tiene de negativo desplazar a un vigilante para comprobar si hay fuego en su vivienda o negocio? Incluso voy más allá: ante una alarma médica, podría practicar primeros auxilios. Todo esto debería analizarse en profundidad y ver cómo queda reflejado en el reglamento”, declaró Jiménez del Castillo.

Para finalizar, Ana Borredá solicitó a los participantes de la mesa su valoración del régimen sancionador, considerado “excesivo”, en tono irónico, por algún ponente. “Lo que sí es cierto es que hay una falta de proporcionalidad en las sanciones”, indicó Pedro de Ibarrodo, cuya opinión fue compartida por Vázquez y Jiménez del Castillo.

## Balance de alarmas

Tras el debate protagonizado por las empresas patrocinadoras, se organizó otra mesa redonda, esta vez para conocer los datos que tienen las FCS sobre esta actividad. Cuerpo Nacional de Policía, Guardia Civil, Mossos d’Esquadra y Ertzaintza aportaron un balance de la evolución de las falsas alarmas en los últimos años y explicaron las acciones

que llevan a cabo con las empresas dedicadas a la atención de las alertas.

El primero fue el inspector jefe del Cuerpo Nacional de Policía Javier Galván, responsable de la Sección de Colaboración de la Unidad Central de Seguridad Privada, que ofreció los datos que posee el Ministerio del Interior en relación con esta actividad. Según informó Galván, actualmente operan en España 114 centrales receptoras de alarmas; menos que las 176 que ofrecían este servicio hace seis años. Para el responsable policial, aunque la desaparición de empresas puede guardar relación con la crisis económica, las causas hay que buscarlas fundamentalmente en "la concentración o absorción de servicios entre compañías".

El número de abonados se sitúa en la actualidad en 1.464.459, con los domicilios como principales clientes (755.493, algo más del 51% del total de usuarios). Son estos últimos precisamente objeto del "delito más acuciante en España, el robo con fuerza en las viviendas".

Entre los datos que ofreció Galván figuraba también el número de falsas alarmas, que suponen "un 90 por ciento" de las que se producen. El año pasado fueron 363.897, si bien las FCS recibieron un total de 35.779 alarmas reales. El inspector jefe de la Sección de Colaboración de la UCSP aseguró que, a partir de 2012, el número de falsas alarmas que recibían los cuerpos policiales disminuyó, a la vez que aumentaban las reales. La razón del cambio se encuentra en la adaptación de las empresas



Javier Galván,  
Cuerpo Nacional de Policía.

a la orden de Interior mencionada por Luis González Pernía sobre el funcionamiento de sistemas de alarma. Esta norma supuso "un aumento de la eficacia y eficiencia del servicio de las CRA y de la respuesta del Cuerpo Nacional de Policía", consideró.

Desde la UCSP a la que pertenece Galván se han puesto en marcha varios procedimientos y protocolos para la comunicación de alarmas, enmarcados en el Plan Estratégico para la Seguridad Privada 2014-2015 del Cuerpo Nacional de Policía, conocido como Securpri. Las iniciativas giran en torno a dos premisas, según apuntó el invitado: "la implicación de la seguridad privada en la seguridad pública y el intercambio de información".

La institución policial está trabajando en estos momentos en procedimientos como el Proyecto Proceda, para que las empresas comuniquen electróni-

camente las alarmas de manera inmediata y con información en tiempo real, o el Proyecto Prisa, que establece un protocolo de respuesta e intervención segura de los agentes policiales ante las alarmas.

## Posibles causas

El teniente coronel de la Guardia Civil José Antonio Montero, miembro del Servicio de Protección y Seguridad (SEPROSE), aportó también datos relativos a las conexiones y alarmas en el ámbito de competencia de la Benemérita. Montero explicó que las conexiones pertenecientes al ámbito de esta institución representan el 20 por ciento del total en España (concretamente unas 275.000).

Este cuerpo de seguridad recibió en 2013 un total de 20.393 alarmas, de las cuales casi un 23 por ciento corresponden a domicilios particulares y más del 17 por ciento a establecimientos obligados. Del total de las alarmas que se comunicaron a la institución, más de un 85 por ciento (17.349) resultaron ser falsas, en su mayoría también procedentes de domicilios particulares y establecimientos obligados.

Aún así, el ponente aseguró que la Guardia Civil no impone un gran número de sanciones. "Tenemos en cuenta las circunstancias del negocio de las CRA y de cada una de las falsas alarmas que se generan", expresó. Por ejemplo, el año pasado hubo 129 propuestas de subsanación y 16 de desconexión por parte de la institución.

Montero coincidió con su compañero del CNP al afirmar que la entrada en vigor de la orden ministerial para los sistemas de alarma provocó un descenso pronunciado de las comunicaciones; especialmente de las falsas alertas, que pasaron de 33.963 en 2011 a 14.353 al año siguiente.

Otro dato interesante que aportó el teniente coronel fueron las alarmas reales que no se comunicaron a la Guardia Civil. En 2013 fueron 624, una cifra inferior al año anterior (634), pero bastante por encima de 2011, cuando dejaron de transmitirse 523 alarmas verdaderas.





Antonio Montero,  
Guardia Civil.

El teniente coronel valoró durante su intervención las posibles causas de las falsas alarmas, de las que tanto las CRA como las empresas instaladoras y los usuarios tienen parte de responsabilidad, desde el punto de vista del SEPROSE. De las primeras, identificó como fallos la falta de información a los clientes y errores de identificación geográfica; en el caso de las instaladoras, se refirió a deficiencias en la instalación, fallos de mantenimiento o sistemas deficientes; y a los usuarios achacó negligencias y desconocimiento de los dispositivos.

Al igual que el CNP, la Guardia Civil ha iniciado en los últimos años diferentes proyectos de colaboración con la seguridad privada que afectan a las compañías que controlan y gestionan alarmas. En 2011 y 2012, la Benemérita lanzó dos instrucciones operativas, una con directrices sobre las comunicaciones de activaciones de alarmas y otra para el tratamiento de las comunicaciones. Además, las centrales de alarmas y centros de control también pertenecen al Programa Cooperar que ha llevado a cabo diversas iniciativas de formación en esta especialidad.

En la recta final de su discurso, Montero anunció que la Guardia Civil ha completado la implementación del sistema Siena, de la compañía Securitas Direct, que "se basa en la transmisión de alarmas por dos vías, correo electrónico y datos a una *tablet*, con imágenes y audio de las alarmas. El opera-

dor tiene así toda la información visual y puede ofrecer más ayuda a las patrullas". Este sistema, puntualizó, no sustituye a la llamada telefónica, tal y como marca la normativa.

## Autonomías

Cataluña y el País Vasco son dos de las comunidades autónomas con competencias en materia de seguridad privada. Las policías autonómicas de ambas regiones conocen bien la problemática de las falsas alarmas porque también han tenido que afanarse en buscar fórmulas que permitan reducir su incidencia. Una de las personas que mejor conoce el impacto de las alertas en Cataluña es Carles Castellanos, subinspector de la Unidad Central de Seguridad Privada de los Mossos d'Esquadra. Según explicó, en Cataluña existen 308.948 conexiones de alarma, una cifra "significativa" que representan cerca del 23 por ciento del total de toda España. De las 101 empresas que trabajan en esta comunidad autónoma, el 80 por ciento de las conexiones está gestionado por sólo una docena de CRA. "Cualquier pequeña variación en alguna de estas 12 centrales va a tener muchísima afectación en los números globales de Cataluña, pero al centrar nosotros la actuación en estas empresas permite que los números vayan relativamente bien", afirmó.

La evolución de las alarmas entre los años 2009 y 2013 ha estado marcada, como en el resto de España, por la aplicación de normativas específicas. La Generalitat de Cataluña aprobó en 2010 una orden autonómica que especificaban los criterios de actuación para el mantenimiento y verificación de los sistemas, así como la comunicación a los Mossos de los avisos. Un año después entraría en vigor la orden ministerial de Interior que afectaba a todo el territorio español; sin embargo, "la orden de aplicación [en Cataluña] es la autonómica y la Estatal tendrá carácter supletorio en aquello que no toque la orden autonómica", aclaró el subinspector.



Carles Castellanos,  
Mossos d'Esquadra.

Aunque se trata de dos normas "sin grandes diferencias", el representante de los Mossos d'Esquadra destacó los "puntos fuertes" de la orden autonómica. Según explicó Castellanos, uno de ellos es que el documento establece un único número de teléfono para que las CRA comuniquen a la Policía de la Generalitat las alarmas, en lugar de que existan varios como sucedía anteriormente.

Por otro lado, la orden contribuye al intercambio de información constante entre las empresas que gestionan alarmas y el cuerpo policial. "Cada 15 días, informamos a todas las CRA de los avisos que hemos recibido y les decimos cuál ha sido el resultado observado por los agentes de policía, si ha habido una intrusión o la consideramos una falsa alarma", aseguró el ponente, quien añadió que la orden establece también deberes a las CRA.

Gracias a esa norma, se aprecia en los últimos años una caída importante del número de falsas alarmas comunicadas a la Policía de la Generalitat. "La realidad es que estamos contentos. Si miramos con perspectiva, de los 90.676 avisos de alarma de 2009 a los 26.338 de 2013, hay una reducción del 71 por ciento", expresó Castellanos. Sin embargo, 2014 es por el momento un bache en esa tendencia a la baja. "Este año los números no están siendo buenos, pero aún así creemos que hay que hablar mucho con el sector antes de empezar a denunciar", sostuvo el invitado.

Al igual que el resto de cuerpos policiales, los Mossos d'Esquadra realizan diferentes actividades con las empresas de seguridad privada, como sesiones informativas, seguimiento de las alarmas, reuniones individualizadas o difusión de consejos y recomendaciones, concluyó Castellanos.

## Formar al usuario

A continuación intervino el comisario jefe de la Unidad de Seguridad Privada de la Ertzaintza, Francisco Llanea, que ofreció el balance de incidencias de falsas alarmas, tanto de los sistemas conectados a una CRA como de los que no, dentro del País Vasco. Aunque Llanea coincidió con el resto de representantes policiales en el descenso de alertas falsas en los últimos años, advirtió que en 2014 la previsión es al alza. "El año pasado, recibimos 6.423 y este año llevamos 4.510 hasta el mes de agosto. De continuar la tendencia actual, se superará la cifra de 2013", apuntó. De hecho, calculó que, de seguir el año con esa evolución, las falsas alarmas comunicadas a la Ertzaintza podrían llegar a las 7.000.

Como el resto de FCS, las falsas alarmas conllevan en ocasiones la sanción por parte de la policía vasca. En 2011 se llevaron a cabo 884 órdenes de subsanación (654), desconexión (135) o reconexión (95), pero sólo un año después, con la orden ministerial en vi-



Francisco Llanea, Ertzaintza.

gor, estos requerimientos cayeron a 329 (263 de subsanación, 41 de desconexión y 25 de reconexión). En 2014, hasta finales agosto se han producido ya 147 requerimientos de subsanación, 36 de desconexión y 18 de reconexión.

Llanea mostró su malestar ante la falta de datos transferidos por parte de las centrales receptoras a la Ertzaintza, que sí llegan, indicó, a otros Cuerpos policiales. "Las CRA no nos comunicáis los contratos que hacéis y, por ello, conocemos una parte del mercado y otra no. Esperamos que con la nueva ley esto se modifique y que se nos comuniquen", expresó ante el público de la jornada.

Entre los principales problemas que observa el comisario de la Ertzaintza en relación con las falsas alarmas des-

taca la "falta de conocimientos" de los usuarios. "La gente no tiene conocimiento de cómo se maneja el sistema ni de las consecuencias que puede traer su mal uso. Nosotros hemos empezado ahora a sancionar a usuarios por el mal uso que hacen de los sistemas de seguridad", aseguró.

Otro asunto que preocupa a la policía vasca es la incidencia de alertas falsas que llegan a través de los pulsadores de atraco. "De las 4.510 comunicaciones de falsas alarmas desde CRA, 618 han sido pulsadores de atraco y códigos de coacción", explicó Llanea. Esta cifra "alarmante" supone un problema porque "lo que se les dice a las unidades policiales es que hay un peligro para la persona y luego resulta que es falso".

La solución a estos dos asuntos pasa por la "formación del usuario en el manejo de los sistemas de seguridad y las consecuencias de un mal uso", según observó el comisario.

Con Llanea finalizó jornada *Servicios de gestión de alarmas: Evolución tecnológica e impacto social*, en la que quedaron patentes los avances que se han producido en los últimos años para reducir la cantidad de falsas alarmas, pero también que el problema no está resuelto todavía. Tecnología, formación de los usuarios y comunicación están entre las principales claves para lograr un paso más. **S**



Foto de familia de directivos de Securitecnia junto a Fuerzas y Cuerpos de Seguridad, ponentes, patrocinadores y presidentes de FES y SEDS.