Boletín Informativo de la
Asociación Española de Empresas de
Seguridad
Número 30 • Octubre 2007

Edición especial

Centrales Receptoras de Alarmas

Dicen que en este mundo de las Seguridades, la premisa de trabajo es fiarnos de todo el mundo y no fiarnos de nadie. Son dos vicios: en el primero se encuentra la virtud y en el segundo la seguridad.

Recientemente se están incorporando nuevas tecnologías en la transmisión de datos por Internet y la pluralización de las instalaciones vecinas a la clásica instalación de un sistema de seguridad, como es el caso de la transmisión de imágenes en tiempo real, ayuda inestimable para los casos de robo, atraco o incendio, en los Centros Receptores de Alarmas. Es necesario hoy en día establecer unos controles continuos en todos los equipos que componen un sistema de alarma así como en los circuitos de comunicación y de inmótica.

Como es natural siempre estamos pensando en las soluciones de las que ya disponemos y que estamos instalando a nuestros clientes. A mi entender, lo que deberíamos es pensar en lo que necesitamos para cumplir con los compromisos que nos demanda el mercado. Las comunicaciones seguras son nuestra asignatura pendiente y creo que es lo que primero se necesita. Lo segundo, la rapidez en estas comunicaciones y continuaremos avanzando.

La nueva normativa EN 50XXX y las especificaciones técnicas en su conjunto vienen a establecer una nueva generación de sistemas electrónicos de seguridad, persiguiendo, como es natural, más efectividad y menos falsas alarmas. Estas normas ya están publicadas y en algunos países de la Unión Europea son de obligado cumplimiento. Con ellas se pretende establecer unas medidas concretas de verificación orientadas a evitar las falsas alarmas y así no desperdiciar recursos bien sean policiales o de las empresas. Es la forma de hacer nuestros sistemas mas eficaces.

Aplicando estas normas, conseguiremos mejorar la calidad en las instalaciones así como en la transmisión y su mantenimiento. La tecnología ha experimentado cambios profundos sobre todo en las comunicaciones, no siendo así en los sistemas instalados, que deberán actualizarse y adaptarse a las Normas Europeas.

Es importante destacar que la clasificación de los riesgos determinará el diseño de la instalación. La clasificación de los sistemas en función al "nivel de riesgo" está suficientemente claro desde el punto de vista que ha establecido la Norma UNE 50131-1, que toma el nivel de capacitación de los delincuentes que supuestamente pueden atacar el sistema.

Es conveniente destacar que también se clasifican de acuerdo con las clases ambientales: dos para elementos exteriores y dos para interiores, aunque no afecte a los niveles de seguridad. Cuanto se expone es muy importante porque los niveles de riesgo son cuatro grados de seguridad: grado 1, 2, 3 y 4.

En el grado uno se supone que los intrusos poseen escasos conocimientos sobre los sistemas de seguridad y pueden emplear una limitada gama de herramientas de fácil adquisición. En el grado dos, los intrusos tienen conocimiento de los sistemas y están dotados de herramientas y equipos electrónicos portátiles. En el grado tres, el conocimiento de los sistemas es bastante alto y la gama de herramientas muy completa. En el grado cuatro, las instalaciones en depósitos de efectivo, valores o metales preciosos instituciones gubernamentales y privadas.

A mi entender la utilidad de un sistema de seguridad electrónico no es de fácil solución porque para que el sistema resulte útil, el tiempo que se necesite para penetrar en el domicilio y perpetrar el delito ha de ser mayor que el de la reacción del sistema. Es decir, el tiempo que transcurre desde que la agresión es detectada hasta que el operador de la Central Receptora de Alarmas decide avisar a las Fuerzas y Cuerpos previa verificación, sumado al que reciben el aviso y se presentan en el lugar de los hechos. Este parámetro puede ser incrementado aplicando medidas físicas.

Las verificaciones de alarmas por las Centrales receptoras. En este momento no existe norma definitiva, pero el proyecto prEN 50138-1 se aprobará el año próximo y aclarará definitivamente todos los procedimientos a seguir con las Centrales de Recepción de Alarmas. No quiero extenderme porque no es Norma definitiva y lo dejaremos para más adelante.

A nuestros clientes y proveedores de equipos de seguridad deberemos concienciarles de que la Seguridad es un proceso, no un producto, y juntos deberemos implantar soluciones técnicas y organizativas que permitan la protección de vidas y bienes, con una visión global y de futuro, ya que las amenazas más importantes, a mi entender, van a venir por las redes de comunicación, tanto para desactivar los equipos de alarma a distancia, o para desde un punto observar las imágenes de toda una organización o la introducción de virus, etc. El enemigo acecha y el reto está echado. Pensemos que un error no se convierte en verdad por el mero hecho de que todo el mundo crea en él. No olvidemos que nuestras decisiones nos hacen ser como somos. Es el momento de, sin perder la fuerza en el presente, poner mucha fe en el futuro y fuerza en el presente.

D. Antonio Ávila Chuliá
Presidente de AES

Boletín informativo de la AES
Octubre 2007 • núm. 30

revista trimestral

Edita:
Asociación Española de Empresas de Seguridad
Alcalá, 99. 2º A
Tel.: 91 576 52 25
Fax:91 576 60 94
28009 MADRID
www.aesseguridad.es
aes@aesseguridad.es

Diseño, realización y edición:
Escriña Diseño Gráfico
Pza. Beata María Ana de Jesús, 13
7º Izq. 28045 MADRID
Tel.: 91 474 37 28
Fax: 91 474 37 11

Junta directiva de la AES

Los servicios de seguridad de atención y acuda. Planteamiento para la eficacia.

El servicio de acuda en la legislación española de Seguridad Privada.

La LSP a través del Reglamento de Seguridad Privada modificado por R.D. 1123/ 2001, recoge la figura de los servicios de custodia de llaves y verificación de alarmas, más conocidos en el ámbito profesional del sector de la seguridad privada como los servicios de seguridad de atención, intervención y acuda.

Las empresas de seguridad privada que sean explotadoras de centrales de alarma, están facultadas al amparo de dicha normativa para "contratar, complementariamente con los titulares de los recintos conectados, un servicio de custodia de llaves, de verificación de alarmas mediante desplazamiento a los propios recintos y de respuesta de las mismas".

La normativa exige que dichos servicios han de ser prestados por vigilantes de seguridad, y consistirán en la inspección del local o locales, y el traslado de las llaves del inmueble del que procede la alarma, con el fin de facilitar a los miembros de las Fuerzas y Cuerpos de Seguridad, posible información acerca de la comisión de actos delictivos así como el acceso al citado inmueble.

La inspección del citado inmueble por parte del servicio de atención inmediata o acuda, debe estar autorizada de forma expresa por sus titulares, habiendo de constar por escrito en el contrato de prestación de servicios firmado entre la empresa de seguridad privada y el propio cliente.

Si bien la legislación exige a las empresas de seguridad privada prestatarias de servicios de custodia de llaves, que estas han de disponer de un armero o caja fuerte que cumpla las características y requisitos establecidos por el artículo 25 de dicha normativa, estas se encuentran facultadas a su vez para que las llaves se encuentren custodiadas por vigilantes de seguridad sin arma en automóvil y conectados por radioteléfono a la CRA, siempre y cuando resultara conveniente para la empresa y los servicios policiales, y motivado por el número de servicio de custodia de llaves o por la distancia entre los inmuebles. Se exige para este supuesto que las llaves se encuentren codificadas, debiendo ser los códigos desconocidos por el vigilante que las porta y variando de forma periódica. Todo esto supone una clara ventaja y acercamiento hacia la eficacia en la prestación del servicio al aminorar de forma considerable los tiempos de res-

Suponen una clara ventaja y acercamiento hacia la eficacia en la prestación del servicio al aminorar de forma considerable los tiempos de respuesta

puesta de los servicios de atención e intervención inmediata ante posibles actos delictivos.

No le está permitido al vigilante de seguridad que realiza las funciones de custodia de llaves, simultanearlo con otros servicios. A modo de ejemplo podemos enunciar aquí que un servicio de custodia de llaves y atención inmediata es del todo incompatible desde el punto de vista legal con, por ejemplo, un servicio de rondas o vigilancia periódica.

Procedimientos de actuación.

Al recibirse en la Central Receptora de Alarmas alguna señal de intrusión, fuego, averías, fallos de comunicación periódica del sistema, etc., de un local, comercio o vivienda protegido por un sistema de seguridad el proceso de actuación es el siguiente:

Tras analizar la señal, comprobando si han sido uno o más elementos de seguridad los que han protagonizado el salto, distinguiendo entre elementos primarios y secundarios, se procede a avisar a la propiedad y a las Fuerzas y Cuerpos de Seguridad del Estado.

Tras la llamada de la CRA el personal de la empresa de seguridad acudirá para verificar el salto de la misma y facilitar el paso a las Fuerzas y Cuerpos de Seguridad del Estado

La implantación de un servicio de atención inmediata y custodia de llaves garantiza al cliente que en el caso de saltos de alarma en su instalación provocados por posibles hechos delictivos, averías, o catástrofes tales como fuego, inundaciones, derrumbes, etc., será el propio personal de la empresa de seguridad que custodia su instalación o inmueble quién tras la correspondiente llamada de la central receptora de alarmas, se pondrá en camino hacia el local motivo de la alarma para verificar el salto de la misma y proceder a facilitar el paso a las Fuerzas y Cuerpos de Seguridad del Estado si fuese necesaria su presencia en el lugar, así como a los distintos responsables y/o personal técnico y de mantenimientos si se hubiesen producido daños o averías en la instalación y en su sistema de seguridad.

Este servicio que suele prestarse en muchas empresas con carácter continuo, 24 horas y en otras muchas en horario fuera de la jornada laboral habitual (lunes a viernes de 20:00 a 8:00 y sábados, domingos y festivos 24 horas), supone como ya se indicó con anterioridad una mayor garantía y una rápida respuesta ante situaciones reales de riesgo ocurridas por actos delictivos, problemas técnicos y/o catástrofes.

La gestión llevada a cabo por el servicio de atención inmediata o acuda se ha de ver coordinado y apoyado en todo momento por la Central Receptora de Alarmas, que es quién evalúa la necesidad de enviar el servicio de custodia de llaves a la instalación, coordina sus actuaciones con los responsables del inmueble, Fuerzas y Cuerpos de Seguridad y personal técnico, en caso de que fuese necesario y da por finalizada la actuación en el caso de que se haya verificado que la recepción de señales que motivaron la llamada al servicio de acuda han sido producto de una falsa alarma.

D. Antonio Villaseca López
Consejero Delegado de
Securitas Systems

La problemática del control y gestion de las CRA. Datos estadísticos.

Los actuales programas informáticos para la gestión de alarma, facilitan un perfecto control de todas las señales recibidas en una CRA. Además aportan información complementaria que ayuda al operador en la toma de decisiones a la hora de gestionar.

Las CRA vienen realizando un importante esfuerzo económico para adecuarse a las nuevas opciones

El coste de las comunicaciones ya no es un obstáculo para el cliente. Señales de apertura, cierre, cancelación, test, restauración... se transmiten como norma.

Estos dos hechos unidos a la identificación singularizada de los sensores en las instalaciones de seguridad nos hace concluir que una CRA moderna tiene:

- Una información rápida de cualquier evento.
- Un elevado conocimiento del estado de los sistemas de seguridad.
- Una respuesta fiable en función del análisis de las señales recibidas.

En este sentido las CRA´S vienen realizando un importante esfuerzo económico para adecuarse a las nuevas opciones que este mercado, en continua evolución, nos ofrece.

Con estos mimbres las CRA tienen un índice de filtrado del 92% sobre las señales gestionadas y un 98% sobre las señales recibidas.

A pesar de este elevado porcentaje de filtrado, el hecho de que sólo el 5% de los avisos transmitidos a las FF y CC de Seguridad sean robos consumados puede generar alguna duda sobre la eficacia del sistema.

Los motivos por los cuales se activan los sistemas de seguridad son:

- 80%: Descuido del usuario
- 5%: Alarmas reales
- 3%: Averías
- 1%: Tormentas
- 11 %: Causas desconocidas *

** Aquí se deben incluir los intentos fallidos de robo que no han dejado daños visibles*

Continuamente desde el Ministerio del Interior, se habla de falsa alarma en oposición a alarma real asociando:

• Alarma real = han robado

• Falsa alarma = mala gestión de la CRA.

Sabemos que es muy normal que después de la correcta verificación de una alarma, con aviso a las FF y CC de Seguridad, el resultado final no sea un robo o un atraco.

El conflicto surge porque "NO EXISTE NINGUN PROTOCOLO DE GESTION".

Las herramientas que tenemos para tramitar una señal son:

• **Art. 48 del Reglamento:**

"… verificación con los medios técnicos y humanos de que dispongan y comunicar seguidamente al servicio policial correspondiente las alarmas REALES producidas."

NOTA 1: No se define lo que se entiende por "medios técnicos y humanos".

Es muy normal que después de la correcta verificación de una alarma, con aviso a las FF y CC de Seguridad, el resultado final no sea un robo o un atraco

NOTA 2: No se define lo que se entiende por " alarmas REALES".

• **Art. 50 del Reglamento:**

"…se considera falsa toda alarma que no está determinada por hechos susceptibles de producir la intervención policial."

NOTA 3: No se define lo que se entiende por "hechos susceptibles".

• **Disposición Vigésimo Sexto de la Orden de 23/4/97:**

"… Se considerará prealarma la activación de un elemento secundario del sistema: entendiéndose por señal de alarma la activación del elemento o elementos principales o de más de un elemento secundario."

"Verificada la alarma, las centrales la comunicarán inmediatamente a las FF y CC. de Seguridad correspondientes."

NOTA 4: Sigue sin definirse el término: "Verificada la alarma."

Al definir principales y secundarios (alarmas y prealarmas) se está estableciendo un primer criterio de verificación.

Sin embargo al no existir ningún "PROTOCOLO" estamos a expensas de afirmaciones como:

"No está acreditado que el sensor definido como "PRINCIPAL", protegiera el bien a custodiar" respuesta dada por el Ministerio del Interior a un recurso de una propuesta de sanción por verificación inadecuada.

Nos dicen que una prealarma, al no ser alarma, no se comunicará a las FF y CC. de Seguridad. Por el contrario una alarma tampoco podemos comunicarla si previamente no la hemos confirmado con los medios técnicos y humanos a nuestro alcance que según el Ministerio del Interior deben ser los necesarios para saber si se ha producido un robo o un atraco.

Por otra parte los criterios en la aplicación de la Norma son diferentes en función del cuerpo policial, la Autonomía e incluso la Provincia.

Partiendo del hecho de que no existe ningún sistema que nos garantice al 100% que una alarma es real o falsa, desde AES reivindicamos la urgente necesidad de un PROTOCOLO de gestión que sirva para determinar las pautas que definan qué gestión es adecuada y cuál no la es. Esta es la única manera de unificar criterios y evitar sanciones indiscriminadas y subjetivas.

En esta línea AES ha enviado en numerosas ocasiones sus propuestas al Ministerio del Interior sin resultado positivo hasta la fecha.

D. Francisco Ramos
Director Gerente de
Tecniserv, S.A.

Falsas alarmas Repercusión en los servicios policiales

Los servicios de la DGP, vienen atendiendo diariamente, más de 1.400 señales de alarma, comunicadas por las empresas de seguridad privada. De aquellas sólo un 8%, aproximadamente, resultan positivas (reales), lo que supone un detrimento cualitativo y cuantitativo de la operatividad policial.

A fin de paliar, en lo posible, esta situación, desde la UCSP (Comisaría General de Seguridad Ciudadana), se recomienda a todas las Unidades Provinciales de Seguridad Privada que promuevan el mantenimiento de contactos con el sector de la Seguridad Privada (empresas de Explotación de Centrales de Alarmas y de Instalación y Mantenimiento de Sistemas de Seguridad).

Estos contactos deben ir dirigidos, por un lado a conocer sus problemas y, de forma concreta, los que afectan a una incorrecta verificación de las alarmas transmitidas a las Fuerzas y Cuerpos de Seguridad por las Centrales de alarmas. Por otro lado, concienciar a las empresas de instalación y mantenimiento de sistemas de seguridad, de que una mala instalación de un sistema (por inadecuación del material o el mal seguimiento de su mantenimiento), es causa de la producción de alarmas indeseadas.

Es imprescindible obtener una visión muy aproximada a la realidad del sector y estudiar posibles soluciones

Estas reuniones, además de servir para obtener una visión muy aproximada a la realidad del sector y estudiar posibles soluciones o formas de trabajo, tendrán como objetivo trasladar a los representantes de estas empresas los criterios de actuación de la Administración para conseguir que su actividad de seguridad privada, sea bajo nuestra dirección y control, complemento de la acción policial y no fuente de problemas o derroche de medios humanos y materiales policiales como actualmente ocurre.

En síntesis, debemos insistir en dar solución a causas perturbadoras, en especial las que se derivan de:

- Deficiente verificación de las señales de alarma.
- Comunicación innecesaria a los servicios policiales.
- Sistemas antiguos, de tecnología obsoleta, instalados con deficiencias importantes.

• Sistemas sin mantenimiento o con cuidado deficiente.

• Falta de adaptación a requisitos reglamentarios.

Lograrlo es tarea que compete a empresas, usuarios y Administración, cada uno de ellos en aspectos muy concretos.

Empresas

• Deben asesorar a sus clientes sobre cuál es el sistema adecuado a instalar y a su calidad técnica, de acuerdo con los riesgos a cubrir y con las características físicas del lugar donde va a ser instalado. Es decir, junto a la función puramente comercial de vender, incluso por delante de ella, debe existir una función asesora que sólo busque instalar el sistema más adecuado en cada caso.

• Deben instalar los sistemas, de acuerdo con las disposiciones de la normativa vigente en cuanto a la existencia de elementos primarios y secundarios ya que, en muchas ocasiones, la adecuada protección de los bienes según su valor o exposición al riesgo con la gradación que la norma busca, supone un importante filtro que evita situaciones de falsa alarma y consecuentemente, atenciones policiales innecesarias.

• Deben realizar un adecuado mantenimiento del sistema de seguridad. Deben respetarse las exigencias normativas en cuanto a las revisiones trimestrales o anuales y realizar comprobaciones periódicas de funcionamiento que tengan acordadas con sus clientes, subsanando de inmediato cualquier anomalía que se presente y pudiera producir situaciones de falsa alarma, lo que se traduce en un descenso de situación de alarmas falsas provocadas por un uso inadecuado o negligente del sistema.

Usuarios

Cuando un particular o empresa, sea por mandato legal o propia voluntad, instala un sistema de seguridad electrónico para proteger sus bienes, debe tener muy en cuenta que el fin perseguido, su seguridad, no admite regateos de mercadillo, sino que, por el contrario, exige un concienzudo estudio de las necesidades para poder instalar el sistema más adecuado en cada caso. En este sentido es importante que el cliente tenga confianza en el proveedor de sistemas de seguridad que, como profesional responsable, deberá asesorar a su cliente sobre la instalación que resulte más adecuada y de su funcionamiento.

En resumen, los sistemas de seguridad deben ser vendidos e instalados por profesionales responsables a ciudadanos igualmente responsables.

La Administración:

Representada en este caso, fundamentalmente por el Ministerio del Interior y más en concreto, por el Cuerpo Nacional de Policía, responsable por mandato legal de las tareas de inspección y control del sector de la seguridad privada, sin perjuicio de determinadas competencias que corresponden a la Guardia Civil o a Policías Autonómicas.

Por nuestra parte debemos preparar las patrullas que acuden a las emergencias de forma que tengan conocimiento de los sistemas de seguridad y de sus requisitos reglamentarios que les sirvan para cumplimentar una parte de alarmas que resulta, por los datos que recoge y la información que facilita, verdaderamente eficaz.

La inspección que realicen deberá ser exhaustivo a fin de poder determinar con la mayor certeza posible, si la alarma se activó de forma motivada o fue, realmente, una falsa alarma.

En otras palabras, las reuniones con la empresas de seguridad (centrales de alarmas y de instalación y mantenimiento), deben servir para transmitir un mensaje de colaboración efectiva en la reducción de las falsas alarmas y con ello evitar una actividad policial innecesaria.

Conclusión.

Si la Seguridad Privada ha venido a asumir parcelas de seguridad general, antes exclusivas del Estado, que se concretan fundamentalmente en aspectos preventivos y disuasorios, parece obvio que una operatividad correcta por parte de las Centrales de Alarmas, la instalación adecuada de los sistemas de seguridad y un buen mantenimiento de los sistemas electrónicos y de su cableado, unido a otros instrumentos como son, la presencia de vigilantes de seguridad en lugares de riesgo para personas y bienes; la existencia de determinados blindajes o cerraduras; la recogida de fondos por vehículos acorazados protegidos por vigilantes de seguridad armados o la visión de cámaras de video en el interior o exterior de edificios son elementos que disuaden a los delincuentes para la realización de sus actividades delictivas.

U.C.S.P.

Los sistemas y las características básicas para una adecuada instalación

Qué importante es saber lo que vamos a proteger, o de qué o de quién hay que protegerse. Muy importante también es conocer dónde está ubicado aquello que tenemos que proteger y poder prever cuándo el agresor podría llevar a cabo su amenaza. Es importante porque cuando disponemos de más información, más adecuados son los medios de protección que implantamos y mayor es la posibilidad de elevar el nivel de seguridad de nuestro protegido, ya sea este un bien o una persona.

No cabe duda también de que la elección de unos medios de protección adecuados va a condicionar de manera concluyente la fiabilidad de nuestro sistema. Son sin embargo las dos últimas fases del proceso de implantación de cualquier sistema las que definen la funcionalidad, operatividad y fiabilidad de éste.

Nos referimos al diseño del sistema y a la instalación del mismo. Son muchos los ejemplos que a todos se nos ocurren del fracaso de un sistema por un inadecuado diseño o una deficiente instalación, a pesar de estar formado por equipos y componentes de gran calidad y elevadas prestaciones teóricas.

Analicemos pues cuáles deben ser los criterios determinantes del diseño e instalación de un sistema.

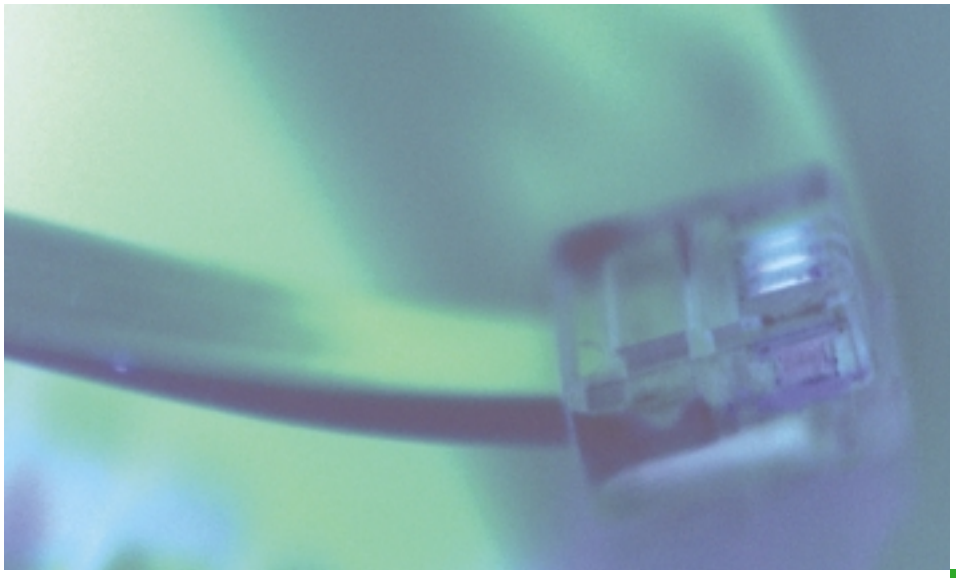
En primer lugar un buen diseño debe contemplar que todas las amenazas y todos los medios empleados han de estar coordinados para conseguir la máxima eficacia en la seguridad. Es clarificador recordar que no es mejor sistema el más sensible, el que más detecta, sino el más fiable, el que detecta aquello que queremos que detecte.

En segundo lugar un buen diseño debe compatibilizar la necesidad de protección con la disponibilidad real de recursos, esto es como vulgarmente se dice: “no matar pulgas a cañonazos”.

Por último, un buen diseño debe contemplar la existencia de un solo centro de control tanto técnica como operativamente. Esto no quiere decir que la información e incluso la gestión del sistema no pueda realizarse de forma distribuida, o que incluso tanto la captación de señales en campo como la posterior gestión de esa información puedan realizarse igualmente de manera distribuida, pero en cualquier caso siempre debe existir una estrategia centralizada con criterios unificados y toma de decisiones únicas.

Un buen diseño implica por tanto profundos conocimientos tanto de los elementos y componentes como de los condicionantes espaciales y temporales, a los que éstos se verán sometidos.

Salvada la fase de diseño del sistema, la instalación completa su implementación. La fase de instalación es la fase pragmática del proceso, la fase en la que se pasa de “las musas al teatro”. La cualificación y profesionalidad del personal que en esta fase interviene define en gran medida su vulnerabilidad. Existen no obstante además de la citada intervención del personal, una serie de criterios que debemos tener en cuenta a la hora de evaluar una instalación.



Estos criterios analizan cada uno de los cinco componentes que cualquier tipo de instalación de un sistema de seguridad posee. Estos son: la Central, los Detectores, los señalizadores, la Energía de Alimentación y las Comunicaciones.

La central de alarmas en cualquier sistema de seguridad es el cerebro del sistema, el componente que analiza, discrimina y procesa las señales provenientes de los detectores y decide la transmisión de aquellas que deben ser informadas como alarmas a través de los señalizadores. La central de alarmas debe ser pues un elemento especialmente protegido e incluso autoprotegido, de igual forma que el cerebro esta protegido por el cráneo que es el hueso mas duro del cuerpo humano, su instalación por tanto así debe asegurarlo.

Los detectores son los elementos encargados de informar a la central de alarma de las variaciones del efecto supervisado. Es fundamental que su instalación sea realizada teniendo en cuenta su principio de funcionamiento y que el área de detección analizada sea correctamente delimitada y programada. La actitud, la ubicación, el alcance y la orientación del detector determinarán en gran medida la fiabilidad del sistema, en muchos casos para optimizar la fiabilidad del sistema se requerirá además un ajuste de sensibilidad.

Este será el caso de los sistemas de detección en exteriores, también denominados sistemas de detección perimetral donde la influencia de las condiciones ambientales, climatológicas y orográficas pueden suponer una importante fuente de generación de señales de alarma. En estos sistemas la interpretación de las señales cobra una especial relevancia, en efecto no todas las señales de alarma generadas "serán susceptibles de intervención policial" sin que por ello deban ser consideradas como "falsas alarmas".

No es mejor sistema el más sensible, el que más detecta, sino el más fiable, el que detecta aquello que queremos que detecte

En muchos de estos casos será preciso por tanto establecer el compromiso entre sensibilidad y fiabilidad, compromiso que en cualquier caso atenderá al nivel de seguridad que se derive del análisis de riesgos.

Los señalizadores serán los dispositivos encargados de comunicar la situación de alarma, detectada por los detectores e informada y calificada como tal, por la central de alarmas. Serán por tanto un elemento igualmente determinante, pues de su correcto funcionamiento dependerá que tengamos conocimiento de que el sistema funciona o no, puesto que ellos serán la interfase del sistema con el exterior. Su ubicación por tanto debe dificultar en la medida que sea posible su fácil manipulación y el canal de comunicación de la información correspondiente debe estar en cualquier caso supervisado y protegido, por los mecanismos que proceda en cada caso en función del citado nivel de seguridad.

Igualmente las comunicaciones entre los detectores y la central, deben ser supervisadas además de seguras en cualquier caso, debiendo garantizar la integridad de la comunicación sin posibles intrusiones externas. La posible interceptación o sabotaje de estos canales, especialmente en las comunicaciones inalámbricas, cobra una vital importancia en nuestros días constituyendo en sí mismas un subsistema de seguridad subyacente.

Por último y no por ello menos importante la energía de alimentación debe garantizar el funcionamiento de manera continua y segura de todo el equipamiento que compone el sistema de seguridad. Como componente básico de cualquier sistema, la energía eléctrica que se debe disponer contemplará sistemas alternativos "de seguridad", que en supuestos de cortes en el servicio habitual garanticen de manera inmediata y sin perdida de control, la continuidad del servicio.

Un buen sistema de seguridad debe por tanto implicar además de un buen producto y un adecuado procedimiento, un estudiado diseño y una delicada instalación. La integración de estos cuatro importantes factores definirá de manera determinante el nivel de seguridad que queramos adoptar, así la elección de un buen producto si no está respaldado por un adecuado procedimiento, diseño e instalación no garantiza nada. El mismo resultado obtendríamos si partiendo de un buen diseño y una buena instalación de un sistema, no seleccionamos un producto adecuado.

Al igual que ocurre con el eslabón más débil de una cadena el factor menos cuidado será el que condicione el nivel de seguridad de nuestro sistema de seguridad.

D. Julio Pérez Carreño
Director Dpto. Sistemas
de Eulen Seguridad

La calidad en el servicio de las CRA su personal y formación especializada

Formación: la primera clave para asegurar la calidad del servicio

Una empresa de servicios es aquella que orienta su actividad a satisfacer ciertas necesidades o deseos concretos de la sociedad. En este sentido, las empresas de seguridad privada no dejan de ser una variante específica de empresa de servicios, ya que satisfacen una necesidad social muy concreta: aportar seguridad.

La parte de la sociedad que precisa y contrata a una empresa de seguridad, y que por tanto recibe un beneficio directo a través del servicio recibido, son los clientes. No obstante, conviene no olvidar, aunque no sea objeto de este artículo, que las empresas de seguridad aportan otros beneficios sociales importantes, tales como la cooperación con la seguridad pública, la reducción de la siniestralidad, la colaboración en la contención de la delincuencia, la generación de riqueza y empleo, etc.

Por tanto, la actuación de toda empresa de seguridad debe centrarse, como en cualquier empresa de servicios, en la atención al cliente. El cliente es el centro y la razón de ser de la actividad empresarial. Y cuidarle y atenderle adecuadamente debe ser el objetivo principal.

Entre las diferentes actividades que pueden desarrollan las empresas de seguridad, la de Central Receptora de Alarmas (CRA) es una de las que tiene una mayor interacción con los clientes. Por ello, todo esfuerzo realizado para que el nivel de calidad de los servicios prestados a los clientes desde la CRA sea lo mas elevado posible tendrá un enorme valor.

La principal herramienta para lograr ese objetivo de calidad se llama formación. El personal operativo podrá desempeñar el servicio con el nivel de calidad que pretendemos, en vez de realizar gestiones de mero trámite, únicamente si está adecuadamente formado y sensibilizado respecto a la excelencia en la atención al cliente.

Los planes de formación y la importancia de procedimentar

Para conseguir que el personal operativo de una CRA gestione adecuadamente cualquier alarma, incidencia o situación telefónica, es preciso que conozca previamente las situaciones habituales y las dificultades a las que se puede enfrentar, debemos dotarle de los conocimientos, procedimientos y herramientas técnicas necesarias para desempeñar bien su labor. Un primer paso será organizar adecuadamente la formación operativa que deseamos impartir, estructurándola previamente en planes de formación y procedimientos de actuación. Respecto a los planes de formación deberemos contar al menos con los siguientes:

• Plan de formación inicial: constituido por todos los temas y procedimientos que es necesario dominar para iniciar la actividad operativa. Se deberá incidir tanto en aspectos técnicos como en los de atención al cliente.

• Plan de formación continua: los realizados periódicamente para mantener y mejorar la formación inicial. Se incluirán prácticas con la revisión de tramitaciones significativas llevadas a cabo para su análisis en común.

• Plan de simulacros: simulación de incidentes reales y de situaciones de crisis para ensayar la respuesta ante diferentes tipos de emergencia.

Además, para optimizar los recursos humanos desde una perspectiva de calidad es también absolutamente necesario procedimentar y definir los procesos de actuación:

• Definir con procedimientos o flujogramas la actuación ante cualquier tipología de llamada, alarma o incidencia recibida.

• Tipificar las situaciones o preguntas clave que puedan exponer los clientes para tener definida la respuesta del máximo número posible de actuaciones estándar o repetitivas.

• Definir procesos relacionados con tareas administrativas relacionadas con la actividad.

La imagen de nuestra empresa dependerá de la formación

Una CRA no deja de ser un “Call Center” o Centro de Atención Telefónica muy especializado. Es sabido que cualquier “Call Center” constituye la primera línea de servicio en la atención al cliente, contribuyendo activamente a formar y mantener la imagen externa que nuestra empresa transmite.

Desde la CRA se producirán constantemente lo que se denominan

momentos de contacto. Los momentos de contacto son aquellos en los que se produce una interacción con el cliente y durante los cuales se pone a prueba una y otra vez la imagen que obtiene de nuestra empresa. Tras cada momento de contacto esta imagen puede salir reforzada o deteriorada. Por ello, es muy importante que estas interacciones sean percibidas por el cliente como de alta calidad. Y la calidad dependerá únicamente de la adecuada formación y motivación del personal operativo que atienda al cliente.

Calidad significa rentabilidad

Cuando el personal operativo no tiene claros los conocimientos precisos para desempeñar su labor o no disponen de los procedimientos y manuales que les marquen claramente las pautas a seguir, además de aumentar el riesgo de cometer graves errores, necesitarán más tiempo para gestionar cada llamada, cada alarma o cada incidencia, lo que afectará a su nivel de efectividad y, por ende, a su productividad. Por tanto, una falta de formación conllevará, sencillamente y entre otras posibles consecuencias, una pérdida directa de rentabilidad. Es el coste de la no calidad. Y por el contrario, cualquier mejora en el nivel de la calidad del servicio mejorará directamente su eficacia, su producción y, por tanto, nuestra rentabilidad.

Actualmente las CRA, como en cualquier otro tipo de "Call Center" y quizás derivado de su atención permanente durante las 24 horas, absorben cada vez en mayor medida una parte muy importante del tráfico telefónico de las empresas de seguridad. Por ello, aprovechando esta circunstancia debemos evolucionar y adaptarnos para convertirla, con la formación adecuada del personal, en una oportunidad de generar nuevo negocio y una ayuda para reducir costes. Mediante una adecuada atención telefónica las CRA pueden reconvertirse en lo que podemos denominar Centros Multiservicios:

• Se puede conseguir nuevo negocio asesorando al cliente "en caliente" ante cualquier demanda de información comercial sobre otros productos o servicios de la empresa sobre los que muestre interés o se lo sepamos crear.

• Se puede colaborar de múltiples formas en la reducción de costes, como por ejemplo evitando intervenciones técnicas presenciales innecesarias, actuando como help-desk (soporte técnico), resolviendo sobre la marcha quejas y reclamaciones, resolviendo directamente las solicitudes de modificación de datos administrativos, etc.

Controles de calidad: evaluación constante del nivel de servicio

Una vez alcanzado un buen nivel de calidad en el servicio hay que luchar para mantenerlo de forma estable con el paso del tiempo. Para ello es necesario aplicar un método continuo de evaluación y perfeccionamiento a través de controles de calidad. Los controles de calidad permitirán revisar frecuentemente el nivel de cumplimiento de los estándares de calidad que nos hayamos marcado, tanto en la atención y el trato telefónico en situaciones de normalidad como en la capacidad de resolución de incidencias.

El objetivo será detectar áreas de mejora sobre las que plantear planes de actuación muy concretos. Estos planes de actuación deberán contar con tres aspectos claramente definidos: el objetivo que se pretende, la metodología para llevarlo a cabo y la planificación en el tiempo para su consecución.

Asimismo deberán existir métodos para medir el nivel de satisfacción de los clientes respecto a los servicios recibidos, los cuales no dejan de ser controles de calidad muy específicos para medir el nivel de los servicios que prestamos. Una forma sencilla de hacerlo será mediante breves cuestionarios telefónicos.

También será necesario realizar periódicamente una revisión de los procesos (consultoría de procesos) que permitirá conseguir un doble objetivo:

• Definir nuevos procesos necesarios para desarrollar adecuadamente el servicio.

• Evaluar la aplicación de los existentes para recomendar su redefinición o la aplicación de planes de reciclaje o mejora continua que permitan optimizar el nivel de calidad de los

servicios y, como consecuencia, seguir mejorando su rentabilidad.

La selección

Con independencia de que uno de los pilares básicos de la calidad del servicio estará basado en la formación del personal operativo, podremos avanzar mucho si previamente lo seleccionamos adecuadamente. A la hora de seleccionarlo deberemos tener en cuenta aspectos como la formación académica aportada, un adecuado nivel de cultura general, una buena capacidad de expresión oral, conocimiento de idiomas si precisamos que el operador sea multilingüe, y otros aspectos relacionado con su personalidad y actitudes que, preferiblemente, deberán ser evaluados por profesionales capacitados. El objetivo será desde un primer momento obtener especialistas. La unión de una buena selección con una adecuada formación nos permitirá lograrlo.

Incentivación de la experiencia

No hay nada más valiosos en una CRA que un operador experimentado. Y esta experiencia debe recompensarse adecuadamente, tanto económicamente como con otro tipo de incentivaciones.

Una buena forma de potenciar la experiencia es implantando lo que podemos denominar como la carrera profesional del operador. La carrera profesional será una visión facilitada desde el primer instante al operador de la evolución profesional que puede obtener a largo plazo. Los factores a combinar deberán ser como mínimo los siguientes:

- La definición de la escala de categorías que se decida implantar.

- Los momentos en el tiempo en los que se podrá acceder a un cambio de categoría.

- Los niveles salariales que acompañarán a cada categoría.

- Los conocimientos predefinidos que deberán haberse adquirido para optar dicho cambio.

- La evaluación positiva deberá ser probada mediante exámenes de los nuevos conocimientos requeridos.

- Y la evaluación positiva deberá venir acompañada de una valoración igualmente positiva de los responsables directos respecto a aspectos relacionados con la actitud del operador aspirante a un cambio.

El resultado será una tabla que cruzará las diversas categorías existentes, el nivel salarial asociado a cada categoría, el tiempo de experiencia necesario para acceder a la siguiente, los cocimientos necesarios para optar a cada cambio, etc. Este sistema persigue un único fin: fidelizar a la plantilla experta mediante un sistema justo de valoración y compensación económica progresiva.

Mediante una adecuada atención telefónica las CRA pueden reconvertirse en lo que podemos denominar Centros Multiservicios

La última pieza clave: la motivación

Hay un último aspecto a tener en cuenta a la hora de cuidar al personal experimentado del cual, como ya hemos visto, dependerá la calidad del servicio que prestamos: motivarle.

Motivar no sólo significa compensar económicamente de forma adecuada. La ilusión por el trabajo es la gasolina del talento. El problema de que un operador esté desmotivado no es que se vaya de la empresa, sino que se quede. Es imprescindible derrochar imaginación y proponer iniciativas para que los operadores se sientan valorados. Proponerles nuevos retos o funciones, felicitarles de diversas formas cuando proceda, ayudarles a solventar problemáticas particulares o a conciliar la vida laboral con la vida doméstica, son sólo algunos ejemplos. Fidelizar a los operadores expertos y motivados es invertir en calidad de servicio, lo cual además, como ya hemos visto, redundará en un rendimiento mayor.

Conclusiones

La calidad de servicio en una CRA está en gran medida en manos del personal operativo que interactúa con los clientes. Dicha calidad se sustenta en varios pilares básicos: selección, formación, incentivación de la experiencia y motivación. Los controles de calidad y los planes de mejora continua son también imprescindibles. Con el personal operativo adecuadamente entrenado y motivado podremos transformar nuestra clásica CRA en un Centro Multiservicios que nos ayude a ser más rentables. Debemos evolucionar y adaptarnos a este tipo de cambios. La imagen y el futuro de nuestras empresas dependerán de ello.

D. José Ramón Becerra Fiaño
Jefe de Televigilancia
Fichet Sistemas y Servicios, S.A.
Gunnebo España

El diseño, medios e instalaciones de una CRA hoy. Exigencias, tipos y operatividad de los sistemas.

Tras varias décadas de funcionamiento de las primeras Centrales Receptoras de Alarmas, el estado de la tecnología y de las comunicaciones, el gran incremento de alarmas conectadas así como la presión ejercida para una mejor verificación de las alarmas, debe hacernos replantear el modelo de prestación del servicio que las CRA venían realizando, provocando un cambio sustancial.

No debemos olvidar que las CRA están abocadas hacia un nuevo esquema de funcionamiento que dé respuesta a las nuevas demandas crecientes de los clientes, quienes solicitan un trato cada vez más personalizado. Porque este, es un factor importante de cambio; la concienciación que tienen los clientes hoy en día sobre su seguridad, desde un mejor conocimiento de lo que necesitan, exige de los profesionales un mayor esfuerzo sobre todo en asesoramiento.

Más temprano que tarde, la seguridad tanto del riesgo obligado como del particular, no estará a merced del marketing; saber vender sí, vender mucho por supuesto, pero el servicio se impondrá como el mejor argumento, como siempre.

¿Qué requisitos debe cumplir una CRA del siglo XXI?

COMPONENTES TECNOLÓGICOS

Sistemas de comunicación

Una CRA debe estar preparada para la recepción de comunicaciones en todos los formatos posibles: RTC, telefonía Móvil en todas sus variedades así como vía IP.

Las CRA han dejado de ser receptoras y emisoras de llamadas de voz y datos por vía convencional; ahora deben estar preparadas para recibir voz, datos e imágenes por los nuevos canales que están a su disposición.

Todo ello proporcionando un alto nivel de seguridad en la comunicación y guardando escrupulosamente el cumplimiento de la LOPD.

Hardware y Software

No nos referimos aquí a la compra de mejores y más potentes ordenadores, que también, sino de la implantación de equipos y software específicos.

Cada vez se habla más de la normalización de los sistemas electrónicos de

seguridad y de los protocolos de actuación a seguir por parte de una CRA.

Pero los equipos receptores y el software de gestión de alarmas, por ejemplo, deberían pasar también por el tamiz de la Norma.

Quizás conseguiríamos por ejemplo simplificar esa torre de babel que es hoy en día la existencia de diferentes programas para interactuar con todos los tipos de sistemas que venden los diferentes proveedores (programas de bidireccionalidad); cuánto se simplificaría y se ahorraría en la formación de los operadores si se utilizara un solo protocolo estándar y normalizado.

Integración de sistemas

Hablo desde el punto de vista CRA. Es imprescindible integrar la recepción de las señales generadas desde los diferentes sistemas de seguridad y canales de comunicación utilizados por un mismo cliente: transmisión de alarma convencional, audio y/o video, permitiendo una mayor rapidez en la verificación y tramitación de una alarma.

Componentes organizativos

Una CRA es hoy en día una miscelánea de varios grupos de trabajo, independientes pero a la vez interrelacionados, que abordan misiones diferentes.

El sector de la seguridad tiene un problema común, la falta de personal cualificado; esto es aún más evidente en los operadores de CRA, ya que no existen programas de formación específicos, ni bolsa de trabajo de personal con suficiente experiencia ni una carrera profesional que reduzca la alta rotación.

El primer reto por tanto es la selección y formación de los operadores; el grado alcanzado debe integrarle en una carrera profesional de cara a atender los diferentes servicios y que a su vez reduzca el riesgo de abandono del sector.

Atención al cliente

En la actualidad, aprovechando los nuevos canales de comunicación, existen herramientas cuya finalidad es la de mejorar y agilizar el contacto que nuestro cliente necesite realizar con la CRA permitiendo así que el cliente interactúe de forma limitada con nuestra base de datos para que pueda obtener información de su interés; así los recursos de la CRA se concentran en atender llamadas de emergencia o en la verificación de las alarmas, por ejemplo; un Portal Web Cliente se está convirtiendo en una herramienta imprescindible.

Tramitación de alarmas

Contando con los medios y niveles de preparación adecuados, el operador debe estar preparado para verificar adecuadamente las alarmas. Estamos hablando por tanto de un operador cualificado.

Para reducir el grado de presión y tensión sobre él, ineludiblemente la CRA debe aportar el mayor número de herramientas posible así como una batería de medidas organizativas o protocolos para que esa labor de verificación sea efectiva evitando avisos innecesarios a F.S.E. pero que a la vez no suponga un alto riesgo por falta de tramitación de alarmas reales para su cliente.

Help-Desk o soporte técnico

Se convierte en casi imprescindible la existencia de un grupo que, vinculado a la CRA, pueda resolver incidencias técnicas y asesore a los clientes.

Grupos de mediana y alta especialización

Hoy en día algunas CRA tienen grupos de trabajo diferenciados en función del tipo de cliente (establecimientos obligados como banca, joyerías, etc.) o del tipo de servicio (televigilancia, localización de móviles, etc.).

Debido a la gran presión ejercida por la problemática de las falsas alarmas, podríamos incluir también un grupo dedicado a la prevención, detección y solución de problemáticas por falsas alarmas.

No debemos finalizar este apartado sin referirnos al Protocolo de Actuación elaborado conjuntamente con COESS y EUROALARM que ineludiblemente debe guiar nuestros pasos de ahora en adelante conjuntamente con el resto de normas que deben recogerse sin más demora en nuestra legislación.

D. Jesús Alonso Herrero
Subdirector General Área de
Particulares de Segurcontrol

Boletín Informativo de la
Asociación Española de Empresas de
Seguridad

agradece las colaboraciones que hacen posible esta edición trimestral y anima a todos a que remitan informaciones o artículos de opinión para su publicación

Los operadores y lineas de comunicación y control

Vivimos en una época en que los sistemas de comunicación de voz y datos han revolucionado la vida cotidiana.

Como parte de esa vida cotidiana, la seguridad electrónica tiene una alta dependencia de las vías de comunicación tanto para enviar (cliente) como para recibir (CRA).

Las centrales receptoras de alarmas están obligadas a garantizar la recepción de señales que provengan de los sistemas de seguridad de sus clientes.

Para ello cualquier central receptora debe contar con sistemas de comunicación redundantes:

• Tener varios operadores alternativos que tengan redes de comunicación independientes.

• Operadores que garanticen vías diferentes: líneas cableadas, radio y GSM.

• Centrales receptoras o centros espejo que sirvan de back up.

• Y por supuesto, todos estos medios tienen que venir acompañados de un buen plan de contingencias elaborado conjuntamente con los operadores telefónicos, de tal forma que en caso de incidencia pueda ponerse en marcha un plan de emergencia que evite la interrupción del servicio.

Pero el gran reto hoy en día es asegurar la transmisión de alarmas de los clientes; aunque la tecnología de los sistemas de seguridad sigue basada en el envío de señales a través de RTC, hoy en día se incorporan de forma regular transmisores de telefonía móvil para voz y datos, que permiten una redundancia en las comunicaciones.

Es aconsejable, en contra de la práctica de algunas empresas, que la comunicación, si es posible, sea redundante; siempre que haya línea terrestre, esta debe aprovecharse y reforzarla con la telefonía móvil; basarnos sólo en esta última es correr un alto riesgo dado que el envío de señales de alarma por SMS no está garantizado por las operadoras de móviles.

Las líneas ADSL, en constante crecimiento, nos permiten también una nueva alternativa; utilizando módulos IP se puede realizar una transmisión más rápida y da además un plus de seguridad, ya que puede hacerse un control continuo de la línea telefónica a la que va asociada la ADSL, pudiéndose programar que cada pocos segundos se realice un test de la misma.

La transmisión por IP en seguridad, ya no es cosa sólo de la banca, sino que se está extendiendo cada vez más entre los particulares.

Tanto las ADSL como la transmisión móvil por GPRS o UMTS, abren un importante campo de posibilidades en el envío de la imagen, de tal forma que la vídeo transmisión hoy es un servicio que potencia enormemente las posibilidades de los sistemas de seguridad convencionales, y por supuesto se convierte en una herramienta de verificación.

Pero, para poder dar al cliente el mayor grado de seguridad, hay que ser consciente de cuáles son las debilidades de los sistemas de comunicación.

Es de todos conocida la vulnerabilidad de las líneas telefónicas terrestres que fácilmente pueden ser saboteadas.

La transmisión por telefonía móvil también sabemos que puede interrumpirse con inhibidores, que aunque no se comercializan legalmente esto no ha impedido que puedan ser accesibles para los delincuentes. Además se trata de una red que puede saturarse e impedir que la señal llegue en un corto espacio de tiempo.

Las comunicaciones por IP, realizadas en el entorno de Internet, tienen también el riesgo de ser vulnerables; sólo las redes internas de comunicación de grandes empresas, pueden hacer frente a ataques externos.

Por otra parte debemos tener en cuenta que la cobertura de las líneas de comunicación no abarca todo el territorio; hoy en día todavía existen muchas zonas alejadas de núcleos urbanos, especialmente vulnerables, donde no llegan las líneas fijas ni existe cobertura móvil.

Afortunadamente para estos casos existen las ADSL por satélite que requieren de instalaciones especiales para poder emitir señales hasta la central receptora. Pero este es un servicio costoso y no al alcance de cualquiera.

El alto coste de las comunicaciones en general en España, si lo comparamos con nuestro entorno europeo, es sin duda uno de los grandes obstáculos de la seguridad y sería necesario un abaratamiento de dichos costes para poder ofrecer a los clientes un paquete de servicios que incluya, entre otros, comunicaciones redundantes con el fin de prestar una mayor seguridad de sus bienes y que en la actualidad son rechazados por los clientes por su alto coste.

Tenemos ante nosotros un abanico de nuevas posibilidades, pero queda todavía mucho por hacer; las comunicaciones se han convertido en la herramienta principal de la seguridad pero también es el punto más vulnerable.

Tal vez, a medida que nuestro sector vaya alcanzando un mayor tamaño, podamos llamar la atención de los operadores telefónicos y consigamos que desarrollen servicios y soluciones a medida de nuestras necesidades.

D. Jesús Alonso Herrero
Subdirector General Área de Particulares de Segurcontrol