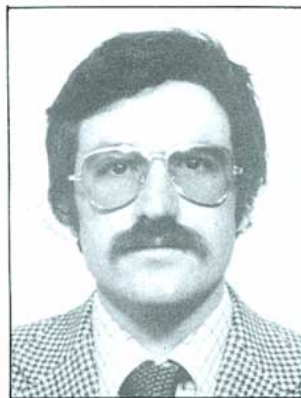


Como ya viene siendo sintomático en este sector, cada vez que se comienza a hablar del mismo para audiencias no formadas únicamente por especialistas, se debe comenzar por aclarar el término "Seguridad".

Sin extendernos esta vez exponiendo la cacareada ambigüedad de la palabra española frente a la pluralidad de términos franceses, italianos o ingleses, debemos recordar que en nuestro idioma "Seguridad" quiere decir "calidad de estar seguro frente a algún riesgo" y que, por lo tanto, hay tantas seguridades como riesgos.

Existe, sin duda, seguridad frente a los riesgos del transporte, por ejemplo, y las tecnologías implicadas afectan a la construcción de firmes de carreteras o a las



Alfonso Bilbao. Director Técnico de Penta III, S.A., presidente de la Comisión de Seguridad del COIT-AEIT, Coordinador de la Subcomisión de Electrónica de la Comisión Técnica 108 (Alarmas) de IRANOR. Lleva 10 años trabajando en proyectos y sistemas de seguridad.

Las Tecnologías de la Seguridad

Texto: Alfonso Bilbao

suspensiones de los automóviles.

En el caso concreto del que trata este artículo, y coherentemente con la dedicación de nuestra Comisión, nos estamos refiriendo a la seguridad frente a riesgos derivados de actos antisociales, esto es, riesgos generados por actividades encaminadas a hacer daños a personas o bienes llevadas a cabo por personas ajenas a los sujetos pacientes de dichos riesgos. Este tipo de seguridad es la que se define en inglés como "security", en italiano como "sicurezza" y en francés como "securite". (Cuadro 1).

1

RIESGOS CONSIDERADOS

- Robo
- Hurto
- Atraco
- Atentado
- Vandalismo
- Sabotaje
- Secuestro
- Espionaje
- Manipulación de Datos

LAS TECNOLOGÍAS DE LA SEGURIDAD

Las Tecnologías aplicadas a la Seguridad son las correspondientes a las medidas que se aplican para obtener seguridad frente a los riesgos mencionados.

Estas medidas se consideran de dos tipos: organizativas y técnicas.

Las medidas organizativas incluyen disposiciones, planes y reglamentos, y no implican tecnología alguna en sentido estricto, si no más bien una cierta metodología de análisis y de organización.

Las medidas técnicas como indica su propio nombre, son las que están afectadas de una aportación tecnológica y, desde el punto de vista del usuario, implican la adquisición de equipos y su consiguiente instalación y mantenimiento.

Las medidas técnicas se han clasificado de forma tradicional en dos grupos, las llamadas medidas pasivas y las medidas activas. (Cuadro 2).

Las medidas pasivas se corresponden con los dispositivos e instalaciones cuyo fin es presentar una resistencia a la materialización del riesgo que se intenta prevenir.

Las medidas activas están formadas por dispositivos e instalaciones cuyo fin es reaccionar ante la materialización de un riesgo en concreto, ya sea de forma automática o como apoyo a la reacción de las personas frente a dicho riesgo.

Si se considera una instalación de seguridad frente a robos en una vivienda, por ejemplo, serían medidas pasivas la puerta blindada, la cerradura de seguridad y las rejas de la terraza, y serían medidas activas el sistema de detección de intrusión (alarma) y la conexión con la empresa de centralización de señales de alarma.

Las medidas pasivas se corresponden con materiales más o menos resistentes a la agresión mecánica (blindajes, cerramientos) y con dispositivos de bloqueo de estos (cerraduras). Por ello las tecnologías implicadas en las medidas pasivas, aún siendo de gran complejidad e interés, no las consideramos adecuadas para ser analizadas en este artículo, ya que no pertenecen a las estudiadas en el ámbito de las Tecnologías de la Información, donde se encuadra el objetivo de esta revista.

Las medidas activas, por el contrario, están formadas por equipos y sistemas plenamente afectados por Tecnologías de la Información, y es su comentario el objetivo último de este artículo. En adelante, cuando nos refiramos a las Tecnologías de la Seguridad, lo estamos haciendo respecto de las medidas activas únicamente.

Estas medidas, dada su

diversidad, pueden subdividirse para su estudio en una serie de Sistemas, que pueden ser los siguientes:

- Detección de Intrusión.
- Control de Atracos y Agresiones.
- Control de Accesos de Personas.
- Control de Accesos de Objetos.
- Vigilancia por Televisión.
- Apoyo a la vigilancia humana.
- Detección de ataques a la información.
- Centralización.

En el cuadro 3 se puede ver la relación entre las medidas enumeradas y los riesgos a los que atienden.

A continuación se analizan brevemente los sistemas expuestos y su evolución, tanto la sufrida como la previsible.

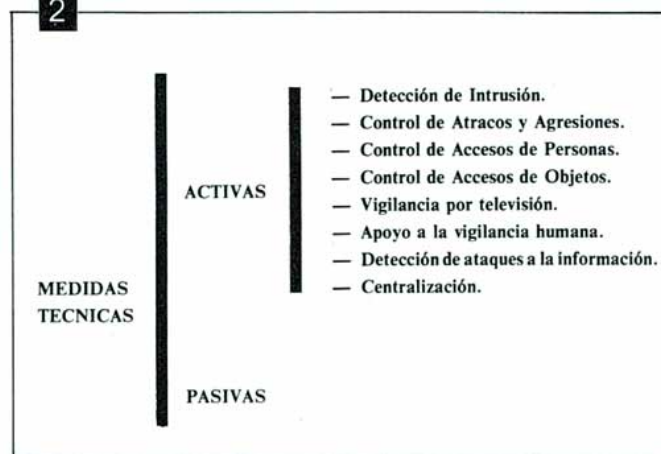
DETECCION DE INTRUSION

Consideramos dentro de estos sistemas fundamentalmente a los elementos sensores de presencia de intrusos.

En el ámbito de las instalaciones en interiores en los últimos años se ha afianzado la utilización de los detectores volumétricos. De entre éstos el más popular es el de detección de radiación infrarroja, cuya sencillez de ajuste y su eficacia, unidas a su precio reducido, han propiciado un elevadísimo consumo de estos equipos en nuestro país, que se estima en unos 40.000 detectores vendidos en 1986.

En instalaciones de riesgo especial se ha popularizado el empleo de detectores de tipo "doppler" de microondas, y en algunos casos detectores piezoeléctricos de vibraciones para muros, suelos y techos.

En las instalaciones en exteriores es donde el reto



3

	Detección de Intrusión	Control de Atracos y Agresiones	Control de Accesos de Personas	Control de Accesos de Objetos	Vigilancia por televisión	Apoyo a la vigilancia humana	Detección de Ataques a la información	Centralización
Robo	X		X		X	X		X
Hurto			X		X	X		X
Atraco		X	X	X	X	X		X
Atentado		X	X	X	X	X		X
Vandalismo	X				X	X		X
Sabotaje	X		X	X	X	X		X
Secuestro		X	X	X	X	X		X
Espionaje	X		X		X	X	X	X
Manipulación de Datos	X		X		X	X	X	X

“

“Hay tantas seguridades como riesgos”.

”

ca), algunos de presión en el suelo y, en los últimos cuatro años, los videosensores, equipos que analizan las señales de vídeo obtenidas desde cámaras fijas de televisión que visualizan las escenas a vigilar.

La utilización a precios cada vez más reducidos de los sensores de utilización en interiores, ha llevado a la popularización de instalaciones de detección de intrusión en viviendas y pequeños comercios, tendencia que va en aumento y que requiere una mayor ordenación por parte del Estado, tanto para evitar las malas instalaciones que generan incómodas consecuencias sonoras como para adecuar la política de aseguración ante robos a la calidad de las medidas dispuestas.

En el sector de las instalaciones en exteriores la evolución ha sido marcada por una mejora en la calidad y eficacia, por lo que cada vez es mayor la incidencia de estos sistemas en los grandes centros industriales, en los recintos militares, centros penitenciarios, centrales energéticas, etc.

En un futuro próximo todo apunta a mantener el incremento de mercado de ambos sectores, el de interiores y el de exteriores.

En el aspecto técnico la tendencia parece ser en los detectores de exteriores el aumentarse la presencia de detectores del tipo videosensor pues el abaratamiento de las cámaras de televisión, la mejora de los algoritmos de análisis de imágenes, el abaratamiento de los dispositivos de digitalización y la tendencia general a utilizar en cualquier caso vigilancia por televisión para comprobar las señales de alarma, hace que la relación de eficacia/costo de estos sensores sea cada vez destacada.

En la detección en interiores se puede destacar la tendencia a minimizarse los tamaños de los sensores, la utilización masiva de volumétricos y la previsible evo-

tecnológico es importante, pues los sensores han de discriminar entre las variaciones ambientales naturales (temperatura, viento, iluminación,...) de las causantes de señal de alarma. Actualmente los detectores más extendidos son los de acople de conductores (precios elevados y no siempre gran efectividad), los de sensibilización de vallados (con las restricciones que esto impli-

lución de éstos hacia la normalización de sus señales, de cara a la integración de las mismas en sistemas complejos de automatización de edificios, ya no siendo señales tipo todo/nada sino que la decisión de si es alarma o no se compare con la historia anterior del detector, la temperatura ambiente, etc.

CONTROL DE ATRACOS Y AGRESIONES

En estos sistemas están incluidos los equipos de aviso voluntario de atraco o emergencia (pulsadores, pedales, pinzas de billetes...) y los elementos de actuación que, en el caso de la comunicación de la señal a distancia se comentan más adelante, y en el de actuación local se concretan en cámaras filmadoras y bloqueos electromecánicos de puertas o mam-paras.

En estos años en España han sido sistemas lamentablemente muy populares, especialmente en entidades bancarias y en farmacias.

Tecnológicamente no presentan ningún tipo de sofisticación, si se exceptúan los sistemas de transmisión de las señales, auténtico punto caliente de estos sistemas.

Socialmente sus consecuencias han sido importantes, sobre todo para el colectivo de los trabajadores de los establecimientos implicados.

En el futuro se prevé una mejora de la eficacia debida a la reducción de los tiempos de comunicación por evolución de las redes entre los establecimientos y las centrales de alarma, y entre éstas y las comisarias y cuarte-lillos de la Guardia Civil, cuyo comentario se hace en el apartado dedicado a la Centralización.

También es de destacar la utilización previsible de cámaras de televisión en grabación continua para el registro de los atracos sin ne-

cesidad de acciones arries-gadas de las víctimas, y para la transmisión de señales de vídeo a distancia para comprobación de falsas alarmas.

CONTROL DE ACCESOS DE PERSONAS

Los sistemas de Control de Accesos de personas son unos de los que más se han ido mezclando con la vida diaria de muchos de nosotros. En realidad están constituidos por elementos que permiten automatizar el control de identidad de las personas para permitir su acceso a algún recinto, función que de forma no automática se viene realizando hace siglos, tanto en la entrada a fortalezas, en la presentación de credenciales, en el paso a una sala de espectáculos (entrada/credencial)...

El desarrollo por un lado de los ordenadores que permiten consultar archivos en breve espacio de tiempo, unido al de las tarjetas con codificación magnética y de otros tipos, ha dejado a las máquinas la tarea de identificar a las personas que han de acceder a los recintos restringidos actuales.

En los últimos años la tecnología ha sido muy activa en su evolución en este campo.

Desde la respuesta cada vez más rápida en la comprobación de los datos de una tarjeta, la capacidad de analizar a un colectivo más amplio o con un número mayor de puntos de control y la dificultad creciente de falsificar las tarjetas, hasta la aparición de los llamados sistemas antropométricos de identificación, como son los analizadores de voz, huellas digitales, iris de los ojos, etc., que permiten rechazar de forma más eficaz las posibles falsificaciones de credenciales o el extravío de las mismas, el avance no ha cesado.

La incidencia de estos dispositivos en el día a día no sólo es importante sino

que crece a un ritmo acelerado. La implantación de medidas de protección frente a la intrusión, tanto pasivas como activas, hace muy necesario garantizar la identidad de las personas a las que se deja acceder a los recintos que se protegen.

En los próximos años se espera una proliferación y abaratamiento de los métodos antropométricos para los recintos de alto riesgo, junto con una estandarización en los sistemas de tarjetas que, como protección ante las falsificaciones caminarán hacia la utilización de tarjetas inteligentes que precisarán alteraciones por parte del usuario de forma periódica (cambios de códigos en lectoras especiales, etc.).

Sin duda veremos cómo la misma tarjeta que nos permite adquirir bienes de todo tipo, nos franquea el acceso a nuestro punto de trabajo y nos sirve de consulta en caso de accidente para conocer nuestro historial clínico.

CONTROL DE ACCESOS DE OBJETOS

Este subsistema agrupa a los elementos de identifica-

ción de objetos que no se han de dejar acceder a algún recinto o frontera. Esos objetos o materiales serán armas, explosivos, drogas, etc.

Las técnicas utilizadas son por un lado las correspondientes a la detección de metales, mediante arco o detector portátil, basado en la variación de un campo electromagnético por la aparición de corrientes de Foucault en los metales a detectar; por otro la detección basada en la inspección visual de valijas y paquetes mediante rayos X y, finalmente, en la detección de la presencia de iones de los explosivos mediante la toma de muestras de los vapores que desprenden ("sniffers").

La aplicación de estos métodos se ha hecho patente para la prevención de ciertos riesgos en concreto como son los de secuestro de aviones, colocación de explosivos en consignas, etc. El respeto de los derechos individuales y el riesgo creciente ha llevado al desarrollo de métodos de inspección de los objetos y prendas personales cada vez más rápidos y eficaces a la vez que menos "ofensivos".

En el futuro se prevé una mayor eficacia en los detectores de explosivos basada en la utilización de técnicas cromatográficas, así como un aprovechamiento mayor del análisis por rayos X basado en la aplicación de técnicas de análisis automático de imágenes.

VIGILANCIA POR TELEVISION

No es preciso explicar en qué consisten los sistemas de vigilancia por televisión en circuito cerrado, si lo es quizá el resaltar la proliferación que de su uso se está constatando en nuestros días.

La tecnología actual parece haber abandonado el avance hacia mayor resolución de imágenes y mejor respuesta a la luz, para concentrarse en llevar hasta los niveles ya alcanzados con

“
La seguridad se entiende cada vez más como un factor de calidad de vida.
”

los tubos modernos, a las cámaras de total tecnología de semiconductores, las llamadas cámaras "sin tubo".

También se nota un gran avance en las técnicas de conmutación, basadas en la aplicación de matrices de conmutación, de tipo microprocesado y modular.

No obstante, el gran avance es la liberación del costoso mantenimiento que va a comportar la nueva tecnología de cámaras, lo que unido a su abaratamiento progresivo hará aún mayor la incidencia de estos sistemas en el mercado.

APOYO A LA VIGILANCIA HUMANA

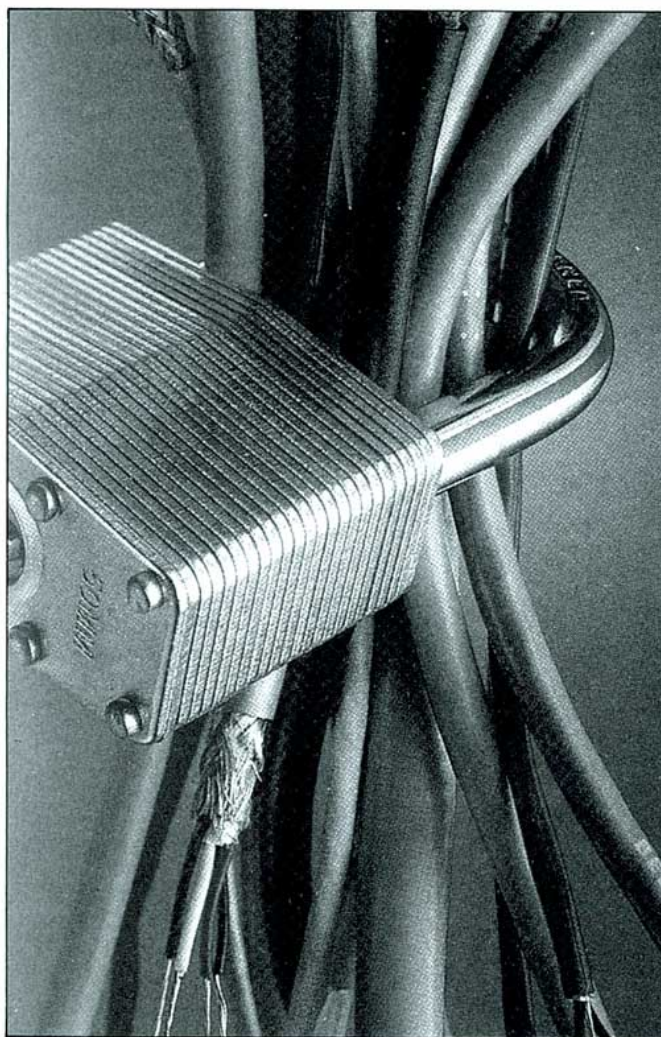
En estos subsistemas hemos englobado los dispositivos de:

- Detección de objetos hurtados en comercios.
- Dispositivos de visión nocturna.
- Equipos de localización de patrullas.
- Equipos de seguimiento de vehículos.
- Radioteléfonos.
- Control automático de rondas.

Su diversidad hace complejo su análisis pormenorizado, sirva esta enumeración para dejar constancia de su existencia y remarquemos que el apoyo de estos equipos y sistemas a las tareas (cada vez más implantadas en nuestra sociedad) de vigilancia de personas y bienes por parte de personal contratado, y también del de la Administración, es creciente, y cada vez más eficaz.

DETECCION DE ATAQUES A LA INFORMACION

Este capítulo es de una especial trascendencia al ser la información, no sólo el objetivo de las tecnologías que agrupan a nuestro colectivo, sino también un bien característico de nuestros días, de valor creciente y,



por tanto, objetivo especialísimo de nuestra seguridad.

Los medios activos de protección de la información afectan a los dispositivos de detección de micrófonos y de transmisores, de una cierta antigüedad, pero es en este capítulo donde debemos referirnos, por excepción, a las medidas pasivas de seguridad, pues en ellas se utilizan técnicas tradicionales de la Tecnología de la Información.

Las más importantes serían las de seccafonía y criptografía de las señales, tanto de voz como de datos, y la utilización adecuada de los Sistemas Operativos de los distintos recursos informáticos, de cara a dificultar el acceso indeseado hasta

donde se halla la información, ya sea para conocerla, sustraerla, alterarla o destruirla.

En el futuro, al menos en España, se espera un importante incremento de las agresiones a la información, pues el nivel de riesgo es aún bajo en nuestro país (parece influir la falta de desarrollo de nuestras redes públicas), por lo que se precisará un incremento de la investigación y el desarrollo en este tipo de medidas.

CENTRALIZACION

Los subsistemas de Centralización cobran importancia en dispositivos de Seguridad de una cierta entidad.

Su estado actual corre parejo al de los subsistemas de control de procesos de otro tipo, por lo que le rigen las mismas pautas de desarrollo: mejora en la calidad de las comunicaciones, incremento de las facilidades para los operadores, auto-diagnósticos y, sobre todo, el reto de la creación de controles automáticos por sistemas expertos.

La incidencia en éstos de condiciones debidas a actuaciones muy diversas de origen humano, dificulta en extremo la creación de un catálogo inicial de situaciones posibles de incidencias.

En otro orden de cosas, pero íntimamente unido a la función de la centralización de señales de múltiples sistemas locales de alarma, se encuentra el problema de la canalización y filtrado de las señales de sistemas privados de alarma hacia los centros de intervención: policía, bomberos, etc. La incidencia en este terreno del estado de las redes públicas y de la legislación vigente en materia de comunicaciones hace que su evolución camine unida a la de estos condicionantes.

COROLARIO

Es muy corto este artículo, y también la capacidad de análisis de su autor, para poder presentar las líneas maestras del pasado tecnológico, del futuro esperable y de la incidencia de ambos en la sociedad con un mínimo de exhaustividad.

No obstante, nos atrevemos a manifestar desde estas líneas que la evolución tecnológica va a seguir su ritmo trepidante también en el sector de la Seguridad, ya que cada vez se entiende ésta no sólo como una necesidad en casos extremos, sino también como un factor de calidad de vida en aquellas sociedades que, por su organización interna de respeto a las libertades individuales, son especialmente vulnerables ante los riesgos enumerados al principio del artículo.