La seguridad industrial en la empresa, hoy

Las tecnologías de la seguridad industrial han registrado un considerable progreso en el mundo entero, y asimismo en España, en apenas diez años. En este espacio de tiempo, el país se ha colocado al nivel de las naciones vanguardistas, y en algunos ámbitos (seguridad hotelera, nuclear y de transportes) se ofrece como un ejemplo a seguir. Cierto que el hurto se ha incrementado por doquier —observándose cooperación internacional—, pero no es menos cierto que los instrumentos para frenar y erradicar semejante delito se han sofisticado aún más. Y ofrecen mejores garantías. Un ejemplo: ya en 1977, tras padecerse en el Reino Unido 120 atracos violentos y sangrientos en centros financieros y de banca, se generalizaron las medidas de seguridad preventiva. Resultado: en 1978, el número de delitos en tal área descendió a 55. Hoy es harto inferior. Huelga señalar que la prevención lúcida resulta efectiva, y no es cara.

Las tecnologías de la Seguridad Industrial han registrado un considerable progreso en el mundo entero, y asimismo en España, en apenas diez años.

DOMINGO PASTOR PETIT

Especialista en seguridad integral.

ATRACO, INTRUSION Y ROBO

Riesgos en común de las empresas: alto valor de las mercancías (en pri-

Los agresores atacan, preferentemente, a las empresas más desprotegidas de la zona. El enemigo ataca en equipo: 2-3 agresores, y a veces más.

meras materias o productos ya elaborados), vasto espacio y peso, cotización en el mercado, y además, cierto porcentaje de empleados amorales o inmorales (fácilmente corruptibles), diversidad de accesos, riesgos de incendio, mayor agresividad y sofisticamiento de los delincuentes, y una ola de terrorismo, sin contar las mafias de creciente expansión.

Perfilemos una cierta motivación del delito contra la empresa:

— Se ataca preferentemente a las empresas más desprotegidas de la zona.
— Se sabe de uno o varios quintacolumnistas empleados en la industria.
— Se ha detectado una cierta indefensión en una determinada área.

Observemos ahora el «rostro» del delincuente:

— Suele actuar en equipo: 2-3 agresores, y a veces más.
— Son personas adultas, profesionales y con experiencia.
— Se sirven para el atraco o hurto de arma blanca o pistolas.
— Antes de la intrusión realizan un frío y completo análisis de los puntos vulnerables de la empresa. Es un espionaje casi perfecto.
— De ordinario cuentan con la ayuda de un quintacolumnista.

Lo más racional que puede hacer el empresario es confiar la salud de su negocio a un médico en tal área, por así decir, o sea, un experto en Seguridad Integral. A éste se le exigirá un inventario de fallos o vulnerabilidades y una propuesta de soluciones. Recuérdese que la seguridad empresarial es una labor de equipo y no la actividad de unos pocos. Si se quiere evitar o prevenir el atraco, la intrusión y el robo, han de observarse cuatro principios en lo que a defensa pasiva se refiere, y son:

1. **Inmueble.** Su estructura debe ceñirse a unas normas defensivas y no sólo estéticas. Algunas estructuras contienen fallos de raíz, facilitando el acceso y la salida indebidos de personas y productos.

2. **Puertas y ventanas.** Es menester que respondan a criterios de seguridad moderna, con cerraduras y cerrojos sofisticados.

3. **Detectores.** Son precisos no sólo para detectar humos y fuego, sino para denunciar la entrada de intrusos.

4. **Control de accesos.** Merced a modernos sistemas de identificación, con un abanico de medidas coherente con la organización a fin de no coartar la fluidez de movimientos.

Crear un servicio de seguridad, según las proporciones de la empresa, o responsabilizar de aquél a alguien es la medida más sensata y urgente.

El empresario se preguntará: ¿Qué género de riesgos estoy corriendo? ¿Dónde y cómo resulta vulnerable la industria? El costo de unas medidas de seguridad ha de estar en relación directa con el importe de lo que se defiende. Algunas medidas son elementales: reducir el número de accesos, ventanas protegidas con dispositivos detectores antirobo, almacenes y zonas clave bajo la protección de una cámara de televisión, guardias jurados en sitios clave, iluminación diurna y nocturna. Todo ello además de la póliza de seguros por robo y atraco, los sistemas antiincendios y unas normativas de circulación del personal de dentro y fuera, amén de la llamada automática a la policía en caso de agresión. Hasta aquí las medidas visibles y quizá fáciles; ahora abordaremos la gama de medidas de lo que llamamos defensa activa.

DEFENSA ACTIVA DE LA EMPRESA

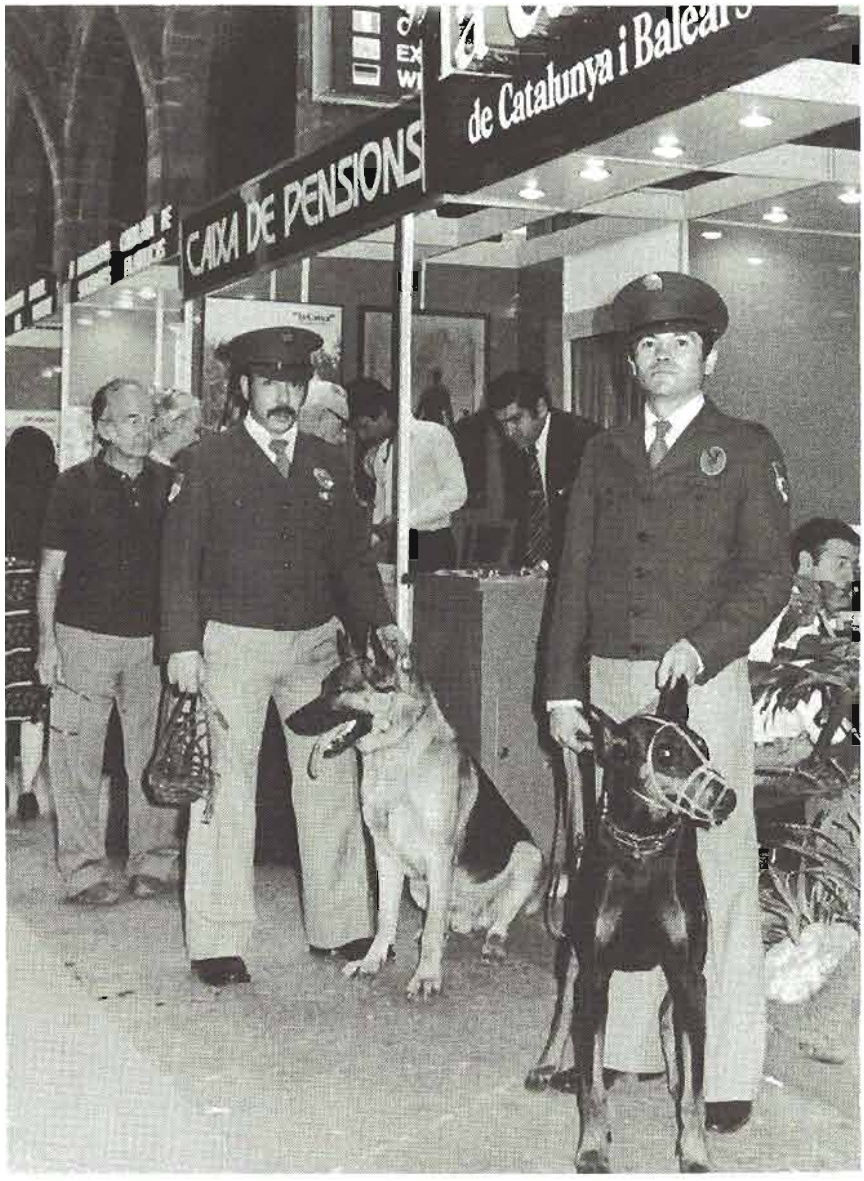
Si esquemático ha sido el análisis de la defensa pasiva, no menos esquemática deberá ser, la descripción de las medidas relativas a la defensa activa. Esta se cifra en la utilización del factor humano. Con el uso de tácticas de protección perimetral y una estrategia operativa en cada área. La defensa activa y pasiva se complementan; no son alternativas, sino complementarias.

Junto a las medidas defensivas, que son visibles, habremos de articular las que actúan de modo invisible. Y debido a que no hay dos empresas parecidas, pues cada una presenta su propia idiosincrasia y su peculiar conflictividad, será preciso ofrecer un cuadro de medidas estándar. La esperiencia ha demostrado que pocos patronos conocen a fondo a todo el personal de su empresa, mayormente cuando ésta sobrepasa los 200 empleados. Y en ese desconocimiento se halla un elemento de riesgo. Si *saber es poder, desconocer significa debilidad.* Es esencial identificar los elementos que pueden presentar riesgo de corrupción (drogadictos, desequilibrados, depresivos, alcohólicos, etc.) a fin de curarnos en salud e impedir forúnculos que podrían degenerar en quintacolumnismo. Véase bien claro que lo que induce al hurto es descubrir las zonas de debilidad empresarial o la capacidad de traición de un operario a un directivo.

Consideremos en un *primer plano* los posibles focos de traición:

— Personal descontento, a veces incluso en altas esferas; es posible que se juzguen mal retribuidos, injustamente valorados.

La seguridad pasiva (inmueble, detectores) necesita de la seguridad activa (factor humano), la seguridad no es alternativa sino cooperativa.



— Personal insatisfecho por causa de rivalidades, falta de ascensos, quizá celos o envidias, y a veces mera inadaptación.
— Personal oportunista y ávido de dinero, carente de escrúpulos y sin sentido de fidelidad a la empresa.
— Personal con ideas políticas revolucionarias, para el que constituye un «deber» ocasionar un perjuicio a la industria.

El número de robos ha sido siempre superior al de los atracos. El robo es más dañoso y grave, y menos fácil, a veces, de aclarar en sus causas.

Cualquier estrategia defensiva se ajustará a estos dos principios:

1. Hay que partir de los medios defensivos de que ya dispone la empresa. Se incentivará la imaginación para hallar soluciones. Toda acción delictiva tiene su base en unas causas y efectos. Eliminar éstos representa una solución momentánea; lo inteligente consistirá siempre en identificar las causas, lo cual será más difícil y espinoso, y a la vez más efectivo.

2. El sistema defensivo propuesto por el asesor en la materia deberá ser analizado por la dirección de la empresa antes de hacer ninguna proposición al Consejo de Administración. Aquella hará sugerencias y juicios de valor, y coherentemente propondrá un presupuesto de seguridad integral. El asesor habrá realizado un chequeo en profundidad.

La seguridad activa consiste en un sistema de protección basado en la utilización de todo el personal de la empresa. Se funda en unos métodos de prevención, protección y vigilancia. Estos métodos se sirven de una organización fluida en la que se contemplan todos los puntos y fases de producción, comercialización, administración, propaganda y venta. Requiere unos controles con más sensibilidad y prudencia que gravosa disciplina, y de ahí que no puedan ser creados a la ligera, sino sopesando los pros y los contras.

INFIDELIDAD LABORAL

Es un fruto intemporal y universal la acción delictiva de un cierto tipo de empleados, y no menos intemporal y antigua ha sido también la explotación. En nuestros días, el director o encargado de una sección suelen quejarse con amargura de absentismo y conductas desleales, amén del pluriempleo. Es sabido, por otro lado, que de nada valen las sospechas ante un tribunal, la magistratura del Trabajo o los sindicatos. En un estado constitucional y democrático se exige el aporte de pruebas y no de suposiciones o meras conjeturas. Ahora bien, ¿de qué manera podemos obtener testimonios fidedignos para demostrar claramente que cierto operario está vendiendo información punta a un competidor del país o extranjero? Estos y otros muchos delitos son el pan de cada día en la totalidad del planeta, y se suceden en todas las épocas y culturas. Porque un cierto porcentaje de personas es asequible al soborno y otras se doblegan ante el chantaje. ¿Qué hacer en forma honesta y efectiva contra ese restringido porcentaje de personas desaprensivas?

Existe un sólo camino y una única respuesta: obtener pruebas del delito. Y aquí se impone el principio bíblico: ser *inocentes como la paloma y, a la vez, astutos como la serpiente*. Es decir: desconfiar por sistema sería torpe política, tan torpe como no desconfiar nunca de nadie. Los griegos solían afir-

Si Al Capone volviera a nacer, sería pirata en los ordenadores y no gangster, pues esto le rendiría al millón por uno.

mar: «A los treinta años, el que no es estúpido se torna el mejor médico de sí mismo.» Aplicado a la empresa podríamos decir: «A los tres años de tener un operario, será estúpido el que no le conozca hasta en su más íntima entraña». Y recuérdese que **saber es poder.**

DELITOS EN INFORMATICA

Si Al Capone volviera a nacer, sin duda sería pirata de los ordenadores y no gángster, pues esto le rendiría al millón por uno. En España se han conocido alrededor de 40 delitos informáticos en los últimos años, y en cada caso se contabilizaron botines no inferiores a los 25 millones de pesetas como promedio. En Europa, EE.UU. y Japón el delito alcanza proporciones aterradoras.

Advirtamos que la seguridad en informática constituye una de las especializaciones más espinosas y complejas —y sin duda más fascinantes— en el marco de la Seguridad Integral. No nos referiremos aquí a los virus informáticos, tampoco al peligro de incendio o inundación, tan sólo abordaremos un bosquejo de la seguridad en este campo, concretamente en un Centro de Cálculo o Proceso de Datos con salas de ordenadores. Aquí nos importa, sobre todo, la seguridad ante hurto, espionaje o sabotaje.

Existen unas homologaciones sobre las instalaciones de alarma contra robo, que son la mejor recomendación al usuario, y tan sólo recordaremos que los locales cerrados y acondicionados deben hallarse dispuestos para un funcionamiento correcto en bandas de temperatura que oscile entre los 0 y 50º C, con un grado de humedad relativa del 60 por 100. Ello no obstante, las condiciones climáticas ideales oscilan entre los 17-19º C. Veamos en síntesis las recomendaciones de orden genérico:

- No situar el ordenador en un sótano ni en un piso elevado.
- Evítense ventanas alrededor, y muy a salvo de agua, fuego, viento, rayos, tensiones y calor.
- Dimensiones no excesivas del recinto.
- El suelo debe ser de piezas desmontables, y los cables, ajustados a normas de aislamiento y seguridad.
- Paredes insonorizadas y de materiales refractarios al fuego y a la humedad.
- El alumbrado y la ventilación circularán por distintos sectores.
- Protección del techo para ponerle a salvo de agentes violentos.
- Las puertas no deben ser más de dos.
- Permanente control con cámaras de televisión.
- Los accesos poseerán detectores de metales.
- Todo el personal del Centro de Cálculo operará bajo un estricto contrato de confidencialidad.
- Riguroso control del material que sale del recinto merced a registro de cintas o discos.
- En caso de recibir visitas —y éstas deben restringirse al máximo— se poseerá una completa identificación de cada visitante.
- Archivos y armarios, con un minucioso control de entradas-salidas de discos.
- Control perenne del número de llaves de acceso.
- Dispositivos de alarma electrónica antirobo.
- La limpieza se realizará bajo el control del responsable de la seguridad del lugar.

Punto clave: responsabilizar de la seguridad de la sala a una persona, y que ésta posea, a su vez, uno o dos ayudantes. Todos ellos asistirán a cursillos de seguridad contra robo, espionaje, sabotaje, incendio, etc. Capítulo especial serán las medidas antifraude, para prevenir y erradicar los peligros de la piratería internacional.

FUGA Y/O SUSTRACCION DE SECRETOS

Lo mismo cuando en un «rifirafe» se hurtan 5.000 millones de pesetas, que cuando se atraca en un tren obteniéndose dos millones y medio de libras esterlinas, hay un denominador común, el espionaje previo. Ninguna operación delictiva importante se lleva a efecto sin que la preceda una minuciosa labor de espionaje. Esta es una realidad cotidiana y mundial.

Según Richard Perle, de la Secretaria de Defensa de los EE.UU., el bloque del Este se ha ahorrado más de 50.000 millones de dólares en los últimos años en investigaciones y ex-

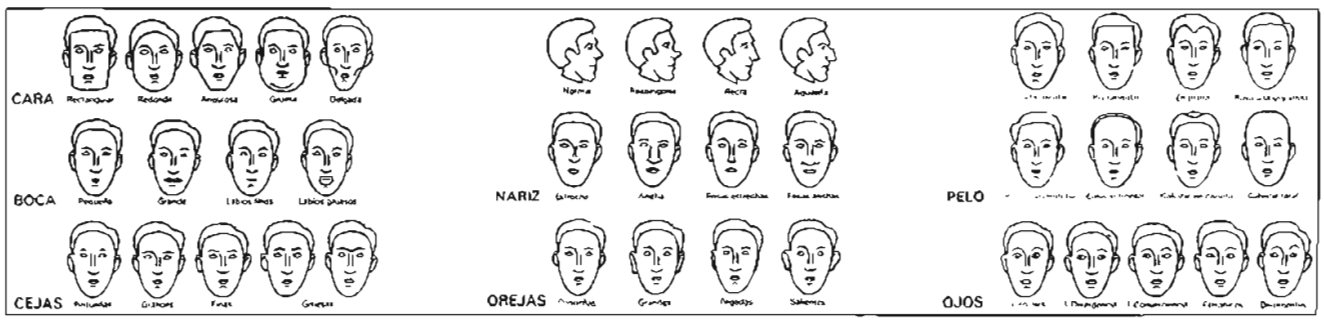
perimentaciones de nuevas armas, a base de hurtar secretos a Occidente.

Nadie crea que siempre ha sustraído el Oriente a Occidente secretos industriales. Recordemos que Europa se hizo con secretos chinos una y otra vez. En el año 552 le espió y robó los secretos de fabricación de la seda; en el 751 hizo lo propio con el papel chino; en el 1250 fue el procedimeinto para elaborar la pólvora; y en el 1710, por medio de un misionero, se hizo con el proceso de fabricación de porcelana. Ya en 1965, los gobiernos de Francia y Gran Bretaña alertaron a sus respectivos empresarios sobre la realidad y el daño del espionaje industrial; cada uno de ambos países lo hizo con la edición de 20.000 folletos.

Dos son los obstáculos para perseguir judicialmente al espía industrial:

- La víctima calla el delito, por cuanto el conocimiento público del mismo supone un desprestigio empresarial. Significa, y no sin razón, que la firma está dirigida con notables fallos, que es débil y vulnerable.

Si saber es poder, desconocer significa debilidad. Resulta esencial identificar los elementos corrompibles.



- El delito del espionaje industrial constituye un problema grave a nivel legislativo por cuanto se halla tipificado en forma endeble o muy ambiguamente. El escollo tiene un marco mundial.

He aquí, a nuestro leal y honesto entender, los principales síntomas de padecer espionaje industrial:

- Se constata la presencia de una entidad publicitaria adelantándose con un producto análogo; raras coincidencias en el enfoque de captación y otros pormenores de parejo contenido.
- El Departamento de Ventas observa de pronto un descenso brusco e injustificado en determinadas áreas. Todo ello en forma irracional e inexplicable.
- Surge la curiosidad agresiva e impúdica de un competidor.
- Se nos piden exhaustivos detalles de un producto, sin el remate de un pedido formal.
- Un especialista nuestro es ganado por la competencia.
- Cierta secretaria opera con exceso de celo y laboriosidad, quedándose sin motivo aparente más horas en la empresa.
- Un técnico se lleva a su domicilio particular ciertas documentaciones para trabajar en ellas, o ése es al menos su pretexto.
- Cierto publicitario decide por su cuenta tomar determinadas fotografías de zonas inaccesibles y especiales.
- Un proveedor o cliente formulan muy concretas preguntas y luego reinciden en torno a ellas con especial ahínco.
- Se registra el extravío o pérdida de una serie de informaciones.
- La persona responsable de la fotocopiadora presenta un número de fotocopias y gastos de papel no justificados ni comprensibles.
- En el ordenador se constatan descuidos (olvido de documentos), además de injustificados retrasos de alguien o incluso el extravío de cintas o discos.

Volvemos a repetir que no hay dos empresas con parecidos problemas, pues cada una presenta rasgos distintos de muy acusada factura. De ahí que no sea prudente facilitar unas mismas recomendaciones para todos. Ello no obstante, vamos a sugerir unos consejos o medidas defensivas ante el peligro, real o próximo, de espionaje industrial. Estas medidas las hemos sintetizado en nueve puntos, y son los que a continuación se afrecen:

- Conviene fijar una clara delimitación en la zona donde se conservan secretos empresariales (fórmulas o procesos de fabricación, listas de clientes o proveedores, acuerdos financieros, fusión entre empresas, patentes y marcas, etc.).
- Sin una rigurosa definición de los secretos empresariales, no puede iniciarse una correcta defensa. Definamos qué son y que no son secretos (comerciales, industriales, tecnológicos, etc.).
- Debe procederse a una estrecha vigilancia —estrecha y sistemática, pero nunca torpe y jamás veleidosa— acerca de las actitudes que pudieran esembocar en el regalo de informaciones. Por ejemplo: en la redacción de folletos, carteles, anuncios, boletines, etc.
- Téngase muy presente el área y módulos de la seguridad pasiva: edificios, disposiciones de alarma, puertas y cerraduras seguras, sistemas de protección interna-externa, vigilantes jurados, etc.
- Perenne reciclaje de las normas de seguridad que rigen para la dirección y ejecutivos. Unos y otros deberán amoldarse a las sucesivas modificaciones.
- Procédase a una protección lúcida y flexible de conferencias y reuniones, que no queden en las pizarras o mesas fragmentos de datos.
- Control telefónico. Sepamos con exactitud que existen como mínimo tres procedimientos para hurtar secretos empresariales, a saber:

  — Desde la compañía de teléfonos, merced a las autoridades y con arreglo a autorizaciones emanadas de un juez.

— «Pinchar» con micros a lo largo de la red telefónica.
— Situar un dispositivo de escucha en la caja de entrada del teléfono.

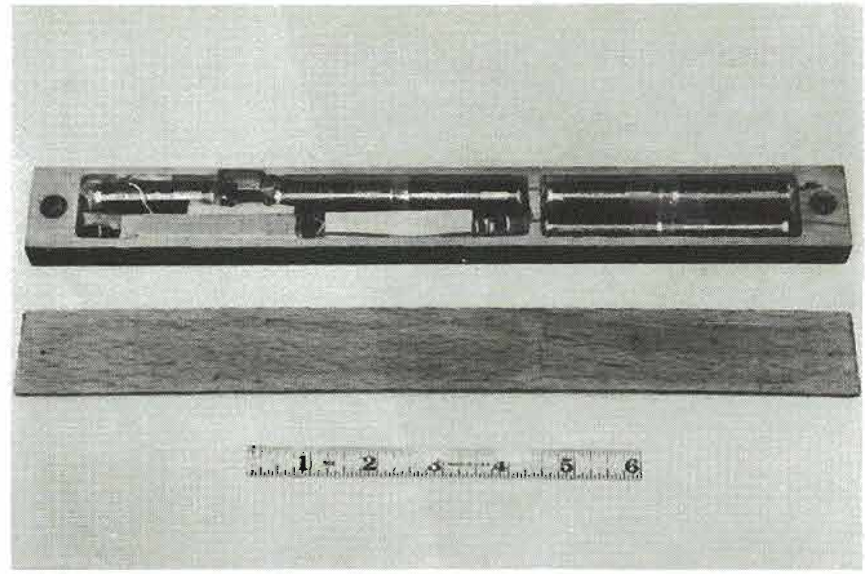
El primero de ellos resulta legal e indetectable, y es legal porque las Fuerzas del Orden Público se reservan el derecho, con tal procedimiento, para identificar a enemigos del Estado; los otros dos procedimientos pueden ser localizados.

• Ante una situación de claro espionaje, caben tres actitudes como respuesta al delito:
— Servirse de la fuente descubierta al enemigo para proceder a una concienzuda y sutil desinformación o intoxicación, según convenga.
— Denuncia del delito a las autoridades competentes.
— Arrancar las pruebas del delito (los micros) y no tomar represalias acaso considerando que la denuncia plantearía problemas de desprestigio empresarial.

• El empresario, ante una incuestionable demostración de haber sido espiado, considerará las ventajas y desventajas de cada una de las tres actitudes anteriores; le convendrá verlas a la luz del tiempo, a la luz del género de represalias posibles. Considerará fríamente las alternativas que se le ofrecen, lo mismo que en una jugada de ajedrez. Y tendrá en cuenta las posibles actitudes y soluciones, las contraofensivas del adversario y las propias defensas posteriores. No cabe actuar sin un análisis de todos los elementos.

LAS EPIDEMIAS DEL TERRORISMO

En el delito se registran algo así como epidemias. ¿Un golpe resulta fructífero para los agresores? De inmediato se produce el consiguiente contagio. Y menudean los delitos semejantes. Unas veces se trata del «rififfi» y otras del «palanquetazo, golpe y patadón». Se han registrado epidemias de cartas-bombas, amenazas e insultos, anónimos, amén de las pintadas (*grafitis*) en los muros callejeros, retretes, calzadas. Los comercios se han llevado siempre la peor parte. Los terroristas, ya se sabe, con sus ritos de sangre, no atienden a razones. A veces el terrorismo resulta imaginativo y audaz, pero en general actúa con una desesperante mediocridad, rutina y carencia de fantasía. Recurre a un arma fácil —el terror, el chantaje, el sabotaje— y se crece ante su propia figura. Se crece, sobre todo cuando



Micrófonos ocultos según un moderno procedimiento.

los medios de comunicación le tratan no como a un ser desequilibrado y paranoico, sino como a un extraño héroe de misteriosa raíz.

Lo peor que le puede ocurrir al empresario que recibe amenazas, insultos o exigencias es intimidarse y perder la serenidad. Si el empresario acierta a conservarse dueño de sí mismo, habrá dado un gran paso. Los terroristas cometen errores, torpezas, sobre todo, cuando no son auténticos terroristas —muy a menudo— sino meros resentidos del área geográfica, enemigos personales de un directivo, o seres inadaptados cuando no embriagados o drogadictos. En el último caso todas sus amenazas y anónimos carece de continuidad, y caen pronto en el vacía. Basta entonces con aguardar y no perder la sangre fría. Caben, empero, algunas de las siguientes medidas preventivas:

• Ante una amenaza de colocación de bomba en algún área de la industria u oficinas, lo más sensato es avisar a la Policía. Ellos tienen especialistas capaces de detectar los explosivos y proceder a la desactivación del artefacto.

• Si se producen reiteradas amenazas por teléfono o se reciben cartas con insultos, convendrá tomar algunas medidas, como, por ejemplo, la creación de un «Comité de Emergencia» integrado por diversos encargados de sección, con un jefe, el cual puede ser precisamente responsable de la seguridad en la empresa. Otra medida sería instruir a la telefonista para que en lo futuro sepa responder al siguiente cuestionario: ¿Edad del comunicante? ¿Cuál es su sexo? ¿Lengua utilizada? ¿Acento regional? ¿Palabras o tacos utilizados? ¿Actitud de cólera, pánico, inseguridad, burla, desequilibrio, amargura, fanfarronería?

• Contactar con las autoridades del lugar y pedirles información de lo que pudiera juzgarse un suceso o una epidemia; presencia de la policía en la empresa algunas veces o acaso de modo regular durante algún tiempo, pues ya se sabe que la presencia de las FOP ofrece un efecto disuasor. Y como en gran número de casos, quizá los más, se trata de sujetos de base enfermiza, no de agresores reales, con tales medidas el hecho no va a más, y se zanja pronto.

• En caso de repetirse las amenazas y producirse explosiones y víctimas, entonces, y previo el consejo de las autoridades, tomar medidas más severas. Algunas de ellas podrían ser: colocación de detectores de metales y explosivos a la entrada de la empresa, adquisición de aparatos detectores de cartas-bombas, vigilancia estricta de personas y coches, registro y detención de sospechosos. Y, por supuesto, extremar la vigilancia, supuesto que la haya, a cargo de los vigilantes jurados.

Las Unidades de Inteligencia son una herramienta de trabajo que permite válidas respuestas a cuatro interrogantes: Tecnología, Mercado, Competencia y Personal.

• Por último, propugnamos la cooperación entre empresarios de una misma zona geográfica. Porque la unión significa fuerza.

El lector recordará quizá que el Grupo Trevi, que reúne a los responsables de seguridad en Europa occidental, aprobó en Madrid en su reunión de Mayo de 1989, la creación de una estructura administrativa supranacional para combatir aunadamente el terrorismo. Esta oficina estará formada por las personas que representan a los diferentes gobiernos. Se acordó en la fecha citada la creación de una Unidad Central de Inteligencia en Europa. Cabe esperar que los frutos de semejante acuerdo serán en el futuro extremadamente fértiles.

LAS UNIDADES DE INTELIGENCIA EMPRESARIAL

Escribió Arnold Toynbee: «La mayor parte de las civilizaciones que han desaparecido se debió a fallos de información. Si un Estado quiere sobrevivir debe estar siempre bien informado.» En la empresa recibe el nombre de Unidad de Inteligencia el órgano empresarial con atribuciones, medios y métodos para acopiar por cauces legales toda cuanta información necesita en torno a los cuatro grandes interrogantes: Teconolgía, Mercado, Competencia y Personal.

Las Unidades de Inteligencia (UI) constituyen una herramienta de trabajo. Nada más y nada menos. Recurrieron a ellas, en primer término, los japoneses en los albores del siglo, y de ahí, en buena parte, el boom de su potencia industrial. Luego se fueron implantando entre las firmas multinacionales de los EE.UU. y Europa occidental. En España son poquísimas las sociedades que disponen de una UI, siendo así que de tenerlas poseerían una información punta capaz de evitar el desfase tecnológico o la dependencia del extranjero y, en todo caso, le ahorrarían al Estado la sangría de ingentes cantidades en royalties; y además, no había industrias obsoletas por causa de tecnología, tampoco habría pérdida de mercados y por ende no se iría a la quiebra. En segundo lugar, las UI permiten un conocimiento absoluto —si bien por medios honestos— de cuanto se cocina en la competencia y en el mercado, y como anexo se poseería una visión penetrante sobre la idiosincrasia y posibilidades de los empleados, con lo que la firma se ahorra sorpresas.

Si la CEE impulso el Grupo Trevi para contrarrestar los daños del terrorismo y a ese Grupo se le ocurrió implantar una UI para combatirlo, significa que tal medida, sofisticada si se quiere, ofrece las cuñas de información con las que vencer los grandes males, aquellos contra los cuales fracasan otras herramientas.

Evidentemente, una UI no opera al modo de una mini-CIA. Las UI no realizan operación alguna que pudiera ser confundida con el espionaje. Sus métodos de trabajo han de ser calificados de sutiles y a la vez simples, honrados y al mismo tiempo audaces. Su objetivo consiste en hacer acopio de grandes masas de información, fieles al principio de la documentación reunida por medio de lo que conocemos como *puzzle*.

La fuentes de información de las UI consisten, fundamentalmente, en el acopio y análisis en profundidad de todo un sinfín de noticias; unas noticias, añadamos, que aparecen en forma dispersa en los medios de comunicación o en fuentes locales y fortuitas. Es decir, que consisten en **reunir y amalgamar datos e información al parecer inconexas, separadas en el tiempo y en el espacio.** Estas noticias, datos, pistas, sugerencias, informes, estadísticas, organigramas o fotos y croquis, aparecen en muy diversas esferas, como, por ejemplo:

- — Ferias y exposiciones.
- — Congresos de Seguridad Integral o Contraespionaje Industrial.
- — Certámenes gremiales a nivel nacional o internacional.
- — Reuniones públicas de base sindical.
- — Revistas especializadas (unas 50.000 en todo el mundo).
- — Prensa en general, además de Radio y TV.
- — Noticias de agencia. Bancos de datos.
- — Representantres. delegados, vendedores.
- — Consultas de los proveedores e intermediarios y transportistas.
- — Peticiones de los clientes.
- — Boletines empresariales.
- — Etcétera.

La UI puede facilitar una respuesta exhaustiva o muy aproximada a la mayoría de interrogantes planteados en cuestiones tecnológicas, estudio del mercado, caminos de la competencia y los procesos evolutivos del personal. Funcionan con pocas personas, necesitan un modesto ordenador y exigen los honorarios que se pagarían a un técnico especialista, no más. El jefe de una UI ha de ser, esencialmente, un profesional dotado de imaginación, curiosidad, agallas y honestidad, y tener un gran conocimiento del producto que fabricamos. Con semejante bagaje, la firma puede emprender un vuelo en verdad ambicioso, y los resultados ser visibles harto pronto, aunque no antes de medio año. A nuestro parecer la adopción de UI es el gran reto a los empresarios con osadía y visión de futuro. ■

BIBLIOGRAFIA

El siglo de la investigación criminal, por Jürgen Thorwald, Editorial Labor, Barcelona, 1966.

Security, por Noel Currer-Briggs, Hutchinson, Londres, 1968.

Les espions dans l'"usine, por Ronald Payne, Libraire Arthme Fayard, París, 1971.

El secreto industrial (know-how), concepto y protección, Editorial Tecnos, Madrid, 1974.

Bancos de datos. Teoría de Telecomunicación, por Roberto Coll-Vinent, Editorial A.T.E., Barcelona, 1980.

Seguridad Empresarial, por D. Pastor Petit, Editorial Mapfre, S.A., Madrid, 1980.

Seguridad Comercial, por D. Pastor Petit, Ediciones Picazo, Barcelona, 1984.

Manual de Seguridad Ciudadana, por D. Pastor Petit, Ediciones Martínez Roca, Barcelona, 1986.